UNIVERZA V LJUBLJANI
FAKULTETA ZA RAČUNALNIŠTVO IN INFORMATIKO

Matjaž Praprotnik

Učinkovito generiranje eliptičnih krivulj za potrebe parjenj

MAGISTRSKO DELO

Mentor: prof. dr. Aleksandar Jurišić

Somentor: doc. dr. Anita Buckley

Ljubljana, 2016

Univerza *v Ljubljani*
Fakulteta *za računalništvo in informatiko*

Večna pot 113
1000 Ljubljana, Slovenija
telefon: 01 47 98 100
www.fri.uni-lj.si
e-mail: dekanat@fri.uni-lj.si

Št.: 154-MAG-RI/2016
Datum: 29. 02. 2016

Matjaž PRAPROTNIK, univ. dipl. mat.

L j u b l j a n a

Fakulteta za računalništvo in informatiko Univerze v Ljubljani izdaja naslednjo magistrsko nalogo

Naslov naloge: **Učinkovito generiranje eliptičnih krivulj za potrebe parjenj**

Efficient generation of pairing friendly elliptic curves

Tematika naloge:

Kandidat v nalogi predstavi parjenja na eliptičnih krivuljah, kriterije in parametre za varno in učinkovito implementacijo ter algoritme za generiranje eliptičnih krivulj za parjenja. Pri tem podrobno razloži osnove teorije eliptičnih krivulj in parjenj. V delu opiše tudi varnostne zahteve in velikosti parametrov. Predstavi primere uporabe parjenj v kriptografji in primere krivulj glede na različne varnostne zahteve. Primere krivulj primerja z obstoječimi standardi in implementacijami. Prispevki naloge naj bodo predstavljene osnove teorije eliptičnih krivulj in parjenj, opis učinkovitih implementacij ustreznih kriptosistemov,pregled zahtevanih varnostnih stopenj za različne scenarije uporabe, opisani algoritmi za generiranje krivulj prijaznih parjenjem v zgornjih primerih, konstrukcija eliptičnih krivulj za uporabo parjenj v posameznih varnostnih okoljih.

M e n t o r:
prof. dr. Aleksandar Jurišić

Fakulteta za računalništvo in informatiko • UNIVERZA V LJUBLJANI • 2

D e k a n:
prof. dr. Nikolaj Zimic

S o m e n t o r:
doc. dr. Anita Buckley

Zahvala

Zahvalil bi se mentorjema prof. dr. Aleksandru Jurišiću in doc. dr. Aniti Buckley za dragocene nasvete, spodbude, predloge in popravke pri pisanju tega dela. Zahvalil bi se moji ženi Tini za potrpljenje, spodbudo in razumevanje ter mojim staršem in bratu za podporo.

Tini

Kazalo

Povzetek

Parjenja na eliptičnih krivuljah so postala zanimiva v zadnjem desetletju, saj omogočajo izvedbo različnih modernih kriptografskih shem in protokolov. Za uporabo parjenj so potrebne posebne eliptične krivulje, katerih konstrukcija zajema področja algebraične geometrije, teorije števil in kriptografije. Zaradi tega so v praksi implementirana v manjšem obsegu, kot bi zaradi uporabnosti lahko bila.

Namen dela je predstaviti eliptične krivulje, parjenja na eliptičnih krivuljah, metode za generiranje parjenjem prijaznih eliptičnih krivulj in priporočila za uporabo in učinkovito implementacijo. Pri tem so podane potrebne osnove iz algebraične geometrije in teorije števil, ki so potrebne za razumevanje tematike.

Delo je sestavljeno iz štirih vsebinskih sklopov razdeljenih v osem poglavij. Prvi sklop dveh poglavij je uvod, v katerem najprej predstavimo zgodovino parjenj na eliptičnih krivuljah in namen dela. V drugem poglavju podamo definicijo parjenj, tipov parjenj in bilinearnega Diffie-Hellmanovega problema. Drugi sklop dveh poglavij predstavljajo osnove algebraične geometrije in eliptičnih krivulj. Tako v tretjem poglavju vpeljemo algebraične raznoterosti in podamo njihove lastnosti. Te predstavljajo osnovo za eliptične krivulje, ki jih podrobneje opišemo v četrtem poglavju. Tretji sklop je namenjen parjenjem na eliptičnih krivuljah. Sestavljen je iz dveh poglavij. V petem poglavju najprej opišemo parjenja na eliptičnih krivuljah in algoritem za njihovo računanje, temu sledi poglavje s primeri uporabe parjenj v kriptografiji. Glavni sklop in rezultat tega dela je v sedmem poglavju, kjer podamo definicijo parjenjem prijazne eliptične krivulje, taksonomijo in pregled znanih metod za generiranje takih krivulj. Eliptične krivulje morajo za učinkovito implementacijo izpolnjevati posebne lastnosti, ki jih naključno generirane krivulje z veliko verjetnostjo nimajo. Za konstrukcijo parjenjem prijaznih eliptičnih krivulj se uporabljajo posebne metode, ki so v delu zbrane in dokazane. V delu podamo tudi priporočila za uporabo metod v različnih scenarijih in možnosti za učinkovito implementacijo. V zaključki navedemo še nekaj odprtih vprašanj na tem področju. V dodatkih so zbrane matematične strukture in lastnosti, ki jih v delu potrebujemo, ter seznami krivulj za predstavljene metode.

Ključne besede: eliptične krivulje, parjenja, parjenjem prijazne eliptične krivulje, asimetrična kriptografija, učinkovita implementacija.

Abstract

Pairings on elliptic curves have become very popular in the decade due to the possibility of implementing modern cryptographic schemes and protocols based on the pairings. For pairings to be effective, special kind of elliptic curves are required. Construction of such curves combines knowledge from algebraic geometry, number theory and cryptography. This is the main reason, that pairings are not implemented as often as they could be.

The purpose of this thesis is to present elliptic curves and pairings on elliptic curves, constructing of pairing friendly elliptic curves and researching their use and efficient implementation. The thesis also contains required preliminaries from algebraic geometry and number theory.

The thesis contains four parts divided in to eight chapters. The first surveys the history of pairings in Chapter 1; Chapter 2 defines pairings, types of pairings and describes bilinear Diffie-Hellman's problem. Algebraic geometry and basic theory on elliptic curves, required for understanding are presented in the second part. It contains definition of algebraic varieties and their properties in Chapter 3 and elliptic curves and their properties in Chapter 4. The third part of the thesis introduces pairings on elliptic curves: Chapter 5 presents pairings and related algorithms, Chapter 6 includes examples of the use of pairings in cryptography. The main part of the thesis is Chapter 7. It includes the definition of pairing friendly curves and all known constructions of pairing friendly curves together with the proofs of these constructions. It also contains recommendations for further implementation and optimization. Conclusion lists some open problems regarding pairings and pairing friendly curves. Mathematical preliminaries required throughout the thesis and examples of pairing friendly curves can be found in the Appendices.

Key words: Elliptic Curves, Pairing, Pairing Friendly Elliptic Curves, Public-Key Cryptography, Efficient Implementation.

Poglavje 1

UVOD

Eliptične krivulje imajo bogato zgodovino in so predmet študija že od devetnajstega stoletja dalje. Uporabljene so bile za reševanje različnih problemov, od razcepa števil do Fermatovega izreka. V tem delu se bomo osredotočili na eliptične krivulje nad končnim obsegom $\mathbb{F}_q$, kjer je q potenca praštevila, dane z enačbo oblike

$$y^2 = x^3 + ax + b, \quad a, b \in \mathbb{F}_q. \tag{1.1}$$

V kriptografiji so se take krivulje prvič pojavile leta 1984, ko je Lenstra [91] opisal algoritem za razcep celih števil, ki uporablja lastnosti eliptičnih krivulj. Leta 1985 sta Koblitz [77] in Miller [104] neodvisno predlagala uporabo eliptičnih krivulj v kriptografiji. Varnost njunih shem temelji na diskretnem logaritmu v grupi točk na eliptični krivulji, ki jo sestavljajo pari $\{(x, y) \in \mathbb{F}_q \times \mathbb{F}_q\} \cup \{\infty\}$. Istega leta je tudi Schoof [132] predstavil prvi algoritem za štetje točk oziroma določanje moči take grupe. S tem je bila postavljen podlaga za uporabo eliptičnih krivulj v praksi. Razvoj algoritmov in shem je hitro napredoval in danes se uporabljajo v veliko standardih in implementacijah.

Nas v nalogi zanima predvsem parjenje na eliptičnih krivuljah. V zadnjem desetletju obstaja veliko zanimanje za to področje. Parjenja namreč omogočajo izvedbo različnih modernih kriptografskih shem in protokolov, kot so šifriranje (Identity Based Encryption - IBE) in digitalni podpisi na podlagi identitete [18, 126], kratki podpisi [21], eno-koračni tripartitni dogovor o ključu [68] in drugi [16]. Veliko navedenih shem in protokolov je bilo v praksi že implementiranih, a za nadaljnjo implementacijo obstaja še veliko možnosti.

Za razliko od standardnih protokolov in shem na eliptičnih krivuljah, (kot so na primer ElGamalovo šifriranje [44] ali ECDSA (ang. Elliptic Curve Digital Signature Algorithm) [39]), kjer za implementacijo uporabimo naključno generirane eliptične krivulje, protokoli in kriptografske sheme, ki uporabljajo parjenja, zahtevajo eliptične krivulje s posebnimi lastnostmi [49]. Te lastnosti so take, da jih naključno generirana eliptična krivulja z veliko verjetnostjo nima. Zato je za implementacijo teh protokolov in shem potrebno učinkovito generiranje primernih krivulj.

Večina kriptografskih protokolov in shem, ki temeljijo na parjenjih, uporablja Weilovo parjenje ali Tate-Lichtenbaumovo parjenje, oziroma kakšno njuno izpeljanko. Vsa taka parjenja vzamejo za vhod par točk na eliptični krivulji E definirani nad končnim obsegom $\mathbb{F}_q$ ali nad njegovo razširitvijo $\mathbb{F}_{q^k}$, ter vrnejo element grupe $\mathbb{F}_{q^k}^*$. Da je shema s parjenjem varna, mora biti diskretni logaritem v grupi točk krivulje E in v multiplikativni grupi

$\mathbb{F}^*_{q^k}$ težko izračunljiv. Če želimo, da bo varnostnim zahtevam zadoščeno, mora biti moč razširjenega obsega znatno večja od reda grupe točk na eliptični krivulji.

Na področju parjenj obstaja že veliko rezultatov. Prvi primeri uporabe so bili namenjeni prevedbi problema diskretnega logaritma v grupi točk na supersingularni eliptični krivulji v problem diskretnega logaritma v končnem obsegu [51, 101]. Praktična uporaba v protokolih in kriptografskih shemah pa se je začela leta 2000, ko je Joux [68] uporabil parjenja za eno-koračni tripartitni protokol dogovora o ključu. Temu so sledile uporabe parjenj za šifriranje in digitalne podpise na podlagi identitete [18, 126], za kratke podpise [21] in za druge namene.

Prvi protokoli so uporabljali supersingularne krivulje, ki pa niso zadoščale vsem varnostnim zahtevam. Zato se je kmalu začelo iskanje primernih krivulj za različne namene. Večina konstrukcij temelji na metodi kompleksnega množenja [2]. Med prvimi sta navadne eliptične krivulje z majhno stopnjo vključitve leta 2001 generirala Cocks in Pinch [34], njima so sledili številni drugi.

Leta 2010 so Freeman, Scott in Teske [49] združili znane konstrukcije eliptičnih krivulj primernih za parjenja in predstavili razvrstitev le teh glede na lastnosti in način konstrukcije.

V nalogi predstavimo parjenja na eliptičnih krivuljah, kriterije in parametre za varno in učinkovito implementacijo ter algoritme za konstrukcijo eliptičnih krivulj primernih za parjenja. Pri tem podrobno razložimo osnove teorije eliptičnih krivulj in parjenj. Opišemo tudi varnostne zahteve in velikosti parametrov ter primere uporabe parjenj v kriptografiji in primere krivulj glede na različne varnostne zahteve. Glavni prispevki naloge so:

- predstavljene osnove teorije eliptičnih krivulj in parjenj;
- opis učinkovitih implementacij ustreznih kriptosistemov;
- pregled zahtevanih varnostnih stopenj za različne scenarije uporabe;
- opisani algoritmi za konstrukcijo parjenjem prijaznih krivulj;
- konstrukcija eliptičnih krivulj za uporabo parjenj v posameznih varnostnih okoljih.

Naloga je sestavljena iz osmih poglavij. Drugo poglavje je uvod v parjenja, kjer definiramo parjenja in predstavimo osnovne lastnosti. V tem poglavju opišemo tudi bilinearni Diffie-Hellmanov problem, ki je osnova varnosti v mnogih protokolih. V tretjem poglavju predstavimo pojme algebraičnih raznoterosti, algebraičnih krivulj ter deliteljev. To poglavje vsebuje številne definicije in izreke s področja algebraične geometrije. Na prvi pogled deluje, kot da vsebina tega poglavja ne sodi v temo naloge, vendar pa je poznavanje tematike potrebno za razumevanje parjenj (še posebej, če nanje ne želimo gledati kot na črne škatle). Tretje poglavje služi tudi kot osnova za teorijo eliptičnih krivulj. Te podrobneje obravnavamo v četrtem poglavju, kjer je poudarek na grupah točk na eliptičnih krivuljah, vključitveni stopnji, razlikami med navadnimi in supersingularnimi krivuljami in kompleksnim množenjem. V petem poglavju opišemo parjenja na eliptičnih krivuljah. Podrobneje predstavimo Tate-Lichtenbaumovo parjenje, Weilovo parjenje, ter algoritem za računanje le teh. V šestem poglavju sledijo primeri uporabe parjenj. Glavni del magistrske naloge je sedmo poglavje, v katerem predstavimo razvrstitev parjenjem prijaznih

eliptičnih krivulj, konstrukcije takih krivulj in predloge za različne varnostne zahteve. Na koncu nanizamo še nekaj odprtih problemov s tega področja. V dodatkih so zbrane definicije in lastnosti polinomov, valuacij in obsegov, ki jih uporabljamo v nalogi. Vse so sicer dosegljive v mnogih referencah, vendar smo jih strnili tu predvsem zaradi bralcev, ki jim ta vsebina ni domača. V dodatku so tudi primeri parjenjem prijaznih krivulj, ki so implementirane v prosto dostopnih knjižnicah.

Poglavje 2

UVOD V PARJENJA

V tem poglavju si bomo ogledali definicijo in osnovne lastnosti bilinearnih parjenj. Podali bomo tudi razvrstitev parjenj glede na vhodne parametre, ki jo bomo uporabili kasneje pri konstrukciji parjenjem prijaznih krivulj. Parjenja bomo definirali na poljubnih grupah. Ogledali si bomo tudi osnovni problem diskretnega logaritma in Diffie-Hellmanov problem (DHP), ter bilinearno enačico slednjega s parjenji.

Naj bo n naravno število. Naj bosta G_1 in G_2 končni aditivni grupi reda n z nevtralnima elementoma 0_1 in 0_2. Naj bo G_3 multiplikativna ciklična grupa reda n z enoto za množenje 1.

Definicija 2.1. Bilinearno parjenje je preslikava

$$e : G_1 \times G_2 \to G_3,$$

za katero veljata naslednji lastnosti:

1. Bilinearnost:
   - Za vsak $P, P' \in G_1$ in $Q, Q' \in G_2$ velja $e(P + P', Q) = e(P, Q)e(P', Q)$ in $e(P, Q + Q') = e(P, Q)e(P, Q')$.
2. Neizrojenost:
   - Za vsak $P \in G_1 - \{0_1\}$ obstaja tak $Q \in G_2 - \{0_2\}$, da velja $e(P, Q) \neq 1$;
   - Za vsak $Q \in G_2 - \{0_2\}$ obstaja tak $P \in G_1 - \{0_1\}$, da velja $e(P, Q) \neq 1$.

V kriptografiji so najbolj pogosto uporabljena parjenja na eliptičnih krivuljah in sicer Tateovo parjenje [148, 146] in Weilovo parjenje [16] ter njune izpeljanke [7, 62, 65]. (Te primere si bomo podrobneje ogledali v poglavju 5). Najprej si oglejmo nekaj enostavnih posledic bilinearnosti.

Lema 2.2. *Naj bo e bilinearno parjenje kot je opisano v definiciji 2.1. Za $P \in G_1$ in $Q \in G_2$ veljajo naslednje lastnosti:*

1. $e(P, 0_2) = e(0_1, Q) = 1$;
2. $e(-P, Q) = e(P, Q)^{-1} = e(P, -Q)$;

3. $e(jP, Q) = e(P, Q)^j = e(P, jQ)$ *za* $j \in \mathbb{Z}$;

4. *Če velja* $e(P, Q) = 1$ *za vsak* $Q \in G_2$ *potem je* $P = 0_1$.

Dokaz. Lastnost 1. sledi iz lastnosti $e(P, Q) = e(P+0_1, Q) = e(P, Q)e(0_1, Q)$ in analogno za Q. Lastnost 2. sledi iz $1 = e(0_1, Q) = e(P + (-P), Q) = e(P, Q)e(-P, Q)$. Lastnost 3. sledi iz lastnosti 1. in 2., lastnost 4. sledi iz definicije in lastnosti 1. ■

Na podlagi oblike in lastnosti grup G_1 in G_2 parjenja razdelimo v štiri tipe [30, 56]:

- **Tip 1**: $G_1 = G_2$;
- **Tip 2:** $G_1 \neq G_2$, vendar obstaja učinkovito izračunljiv netrivialni homomorfizem $\phi : G_2 \to G_1$;
- **Tip 3:** $G_1 \neq G_2$, vendar ne obstaja oziroma ni znanega učinkovito izračunljivega netrivialnega homomorfizma med grupama $\phi : G_2 \to G_1$;
- **Tip 4:** $G_1 \subset G_2$, grupa G_1 je podgrupa grupe G_2.

V primeru, kjer sta $G_1 = G_2$ pravimo da gre za **simetrična** parjenja, sicer pa **asimetrična** parjenja. Kot bomo videli v poglavju 5, večinoma obravnavamo parjenja, kjer sta G_1 in G_2 podgrupi grupe točk na eliptični krivulji.

Za naslednje lastnosti predpostavimo, da je $G_1 = G_2$.

Spomnimo se problema diskretnega logaritma: v aditivni grupi generirani z enim elementom $G = \langle P \rangle$ reda n pri danem $Q \in G$ iščemo tako naravno število $x \in [0, n-1]$, da velja $Q = xP$. Problem diskretnega logaritma za določene grupe, med katerimi so multiplikativne grupe končnih obsegov in grupe točk na eliptičnih krivuljah nad končnimi obsegi, še danes velja za težko izračunljivega [54]. S problemom diskretnega logaritma je povezan tudi Diffie-Hellmanov problem (DHP), katerega bistvo je pri danih aP, bP in P izračunati abP.

Ena od posledic zgoraj naštetih lastnosti bilinearnega parjenja je redukcija problema diskretnega logaritma v grupi G_1 na problem diskretnega logaritma v grupi G_3. Če elementa (P, Q) predstavljata primer diskretnega logaritma v grupi G_1, kjer je $Q = xP$, potem je $e(P, Q) = e(P, xP) = e(P, P)^x \in G_3$. Posledično je $\log_P Q = \log_g h$, kjer sta $g = e(P, P)$ in $h = (P, Q)$ elementa grupe G_3.

Varnost mnogih protokolov, ki temeljijo na parjenjih, temelji na zahtevnosti naslednjega problema.

Definicija 2.3. Naj bo $e : G_1 \times G_1 \to G_3$ bilinearno parjenje. **Bilinearni Diffie-Hellmanov problem** (BDHP) je za dane elemente P, aP, bP, cP grupe G_1 izračunati $e(P, P)^{abc}$.

Težko izračunljiv BDHP implicira težko izračunljiv DHP tako v grupi G_1, kot tudi v grupi G_3. Če bi namreč v grupi G_1 lahko učinkovito izračunali DHP, bi enako veljalo tudi za BDHP v grupi G_3; iz abP namreč s parjenjem $e(abP, cP)$ dobimo $e(P, P)^{abc}$. Podobno velja tudi v primeru, če bi bil DHP problem učinkovito izračunljiv v G_3, kjer bi izračunali $g = e(P, P)$, $g^{ab} = e(aP, bP)$, $g^c = e(P, cP)$ in na koncu g^{abc}.

Po drugi strani pa je odločitveni Diffie-Hellmanov problem (DDHP) v G_1 učinkovito rešljiv, če je le računanje parjenja učinkovito. Pri DDHP se odločamo, ali je dana četverka (P, aP, bP, cP) elementov iz grupe G_1 veljavna Diffie-Hellmanova četverka, tj. ali velja $cP = abP$. To preverimo s parjenji tako, da izračunamo $\gamma_1 = e(P, cP) = e(P, P)^c$ in $\gamma_2 = e(aP, bP) = e(P, P)^{ab}$. Potem je $cP = abP$ natanko tedaj, ko je $\gamma_1 = \gamma_2$.

Podobno kot smo definirali BDHP, lahko sedaj definiramo tudi odločitveni bilinearni Diffie-Hellmanov problem (DBDHP).

Definicija 2.4. Naj bo $e : G_1 \times G_1 \to G_3$ bilinearno parjenje. **Odločitveni bilinearni Diffie-Hellmanov problem** (DBDHP) je pri danih elementih P, aP, bP, Q grupe G_1 in g grupe G_3 preveriti, ali je $g = e(abP, Q)$.

Pomemben rezultat glede izračunljivosti Diffie-Hellmanovega problema je dokazal Verheul [149]

Izrek 2.5. *Naj bosta G in H ciklični grupi praštevilskega reda r in naj bo $e : G \times G \to H$ neizrojeno parjenje. Če obstaja učinkovito izračunljiv netrivialni homomorfizem grup $\Phi : H \to G$, potem Diffie-Hellmanov problem v grupah G in H lahko učinkovito rešimo.*

Dokaz. Naj bo $\Phi : H \to G$ homomorfizem in naj bo $e(P, P) = h$. Potem obstaja tako naravno število c, da velja

$$\Phi(h) = cP,$$

kjer je P generator grupe G. Velja

$$\begin{aligned}
\Phi\left(e\left(\Phi(e(c^{-2}P, aP)), bP\right)\right) &= \Phi\left(e(\Phi(e(P, P)^{c^{-2}a}), bP)\right) && \text{(lema 2.2 (3))} \\
&= \Phi(e(c^{-2}acP, bP)) && \text{(lastnost } \Phi\text{)} \\
&= \Phi(e(P, P)^{c^{-1}ab}) && \text{(lema 2.2 (3))} \\
&= c^{-1}abcP && \text{(lastnost } \Phi\text{)} \\
&= abP.
\end{aligned}$$

Radi bi torej izračunali $c^{-2}P$. Ker je r praštevilo in $r \nmid c$, po malem Fermatovem izreku [150] velja $c^{r-1} \equiv 1 \pmod{r}$ in posledično

$$c^{-2} \equiv c^{r-3} \pmod{r}.$$

Izračunati moramo c^{r-3}, kar lahko naredimo z metodo podobno podvoji in seštej, kjer upoštevamo naslednji lastnosti:

$$\Phi\left(e(P, c^n P)\right) = c^{n+1}P, \quad \Phi\left(e(c^n P, c^n P)\right) = c^{2n+1}P.$$

■

Originalni Verheulov izrek velja za simetrična parjenja oblike $e : G_1 \times G_1 \to G_3$. Karabina, Knapp in Menezes [74] pa so njegov rezultat posplošili tudi na asimetrična parjenja, torej parjenja oblike $e : G_1 \times G_2 \to G_3$. Povzetek njihovih rezultatov je naslednji:

1. Če obstajata učinkovito izračunljiva homomorfizma $\phi_1 : G_3 \to G_1$ in $\phi_2 : G_3 \to G_2$, potem Diffie-Hellmanov problem v grupah G_1, G_2 in G_3 lahko učinkovito rešimo.

2. Če obstajata učinkovito izračunljiva homomorfizma $\phi_1 : G_3 \to G_1$ in $\phi_2 : G_3 \to G_2$, potem je problem diskretnega logaritma v G_2 in G_1 lahko rešljiv v času $\tilde{O}(r^{1/3})$, kar je bistveno hitreje od časovne zahtevnosti Pollard ρ algoritma [120] v času $\tilde{O}(\sqrt{r})$, [1] kjer je r red podgrupe.

[1] $\exists k \in \mathbb{N} : \ \tilde{O}(n) = O(n \log^k n)$.

Poglavje 3

RAZNOTEROSTI, KRIVULJE IN DELITELJI

Glavna tema naloge bodo parjenja na eliptičnih krivuljah. Preden pa si ogledamo eliptične krivulje, jih bomo postavili v kontekst bolj splošnih struktur. Začeli bomo z algebraičnimi raznoterostmi, nadaljevali z algebraičnimi krivuljami in delitelji na krivuljah. Razlogov za uvedbo raznoterosti je več. Glavni razlog je ta, da so eliptične krivulje poseben primer krivulj in s tem algebraičnih raznoterosti. Poleg tega lahko parjenja na eliptičnih krivuljah posplošimo na parjenja na raznoterostih [46, 48, 50] in drugih krivuljah [40]. Teh v nalogi sicer ne bomo predstavili, so pa kljub temu pomembna in uporabna v kriptografiji.

Poglavje je tehnično in vsebuje precej definicij in izrekov brez dokazov. Namen je seznaniti bralca z osnovnimi pojmi algebraične geometrije. Pomembno je predvsem zaradi razumevanja deliteljev in strukture grupe na eliptičnih krivuljah, ki jo bomo obravnavali v poglavju 4. Oboje predstavlja osnovo za parjenja, poleg tega pa poznavanje tematike olajša razumevanje literature. Večina trditev in dokazov je povzetih po [52, 60, 61, 137]. Dolgi in zahtevni dokazi so izpuščeni, lahko jih najdemo v naštetih referencah. Vključeni bodo dokazi, ki še dodatno razsvetlijo, kar želimo povedati.

3.1 Algebraične raznoterosti

Naj bo $\overline{K}$ algebraično zaprtje obsega K, definirano v A.2.3.

Definicija 3.1.1. Množica točk **afinega n-prostor** nad obsegom K je

$$\mathbb{A}^n = \mathbb{A}^n(\overline{K}) = \{P = (p_1, \ldots, p_n) : \ p_i \in \overline{K}, \ i = 1, \ldots, n\}.$$

Množica K**-racionalnih točk** v $\mathbb{A}^n$ je množica

$$\mathbb{A}^n(K) = \{P = (p_1, \ldots, p_n) : \ p_i \in K, \ i = 1, \ldots, n\}.$$

Definicija 3.1.2. Naj bo $\overline{K}[X] = \overline{K}[x_1, x_2, \ldots, x_n]$ kolobar polinomov z n spremenljivkami in koeficienti v $\overline{K}$. Idealu $I \subset \overline{K}[X]$ priredimo podmnožico afinega prostora $\mathbb{A}^n$

$$V_I = \{P \in \mathbb{A}^n : \ f(P) = 0, \forall f \in I\},$$

ki ji pravimo **afina algebraična množica**. Če je V algebraična množica, je **ideal množice** V definiran kot

$$I(V) = \{f \in \overline{K}[X] : \ f(P) = 0, \ \forall P \in V\}.$$

Algebraična množica V je **definirana nad obsegom** K, če je njen ideal $I(V)$ generiran s polinomi iz $K[X]$. Označimo jo z V/K. Če je V definirana nad K, je njena množica K-**racionalnih točk** definirana kot

$$V(K) = V \cap \mathbb{A}^n(K).$$

Za dano algebraično množico V si oglejmo naslednji ideal

$$I(V/K) = \{f \in K[X] : \ f(P) = 0, \ \forall P \in V\} = I(V) \cap K[X].$$

Vidimo, da je V definirana nad K natanko tedaj, ko je

$$I(V) = I(V/K)\overline{K}[X].$$

Naj bo zdaj V definirana nad K in naj bodo $f_1, \ldots, f_m \in K[X]$ generatorji za $I(V/K)$. Potem je $V(K)$ sestavljena iz skupnih rešitev $(x_1, \ldots, x_n) \in \mathbb{A}^n(K)$ polinomskih enačb

$$f_1(X) = \ldots = f_m(X) = 0.$$

Če je $f(X) \in K[X]$ in $P \in \mathbb{A}^n$, potem za vsak element σ iz Galoisove grupe $\mathrm{Gal}_{\overline{K}/K}$ (definirane v A.2.6) velja

$$f(\sigma(P)) = \sigma(f(P)). \tag{3.1}$$

Definicija 3.1.3. Afina algebraična množica V je **afina algebraična raznoterost**, če je $I(V)$ praideal v $\overline{K}[X]$. To je ekvivalentno pogoju, da je $\overline{K}[X]/I(V)$ celostno polje, torej, brez deliteljev niča. **Afini koordinatni kolobar** raznoterosti V/K je definiran kot

$$K[V] = K[X]/I(V/K).$$

Obseg ulomkov kolobarja $K[V]$ označimo s $K(V)$ in ga imenujemo **obseg racionalnih funkcij** raznoterosti V/K.

Če je $f(X) \in \overline{K}[X]$, potem $\mathrm{Gal}_{\overline{K}/K}$ deluje na polinomu f tako, da deluje na koeficientih:

$$\sigma(f(P)) = \sigma(f(\sigma(P)). \tag{3.2}$$

Definicija 3.1.4. Naj bo V afina raznoterost. **Dimenzija** V označena z $\dim(V)$ je transcendentna stopnja razširjenega obsega $\overline{K}(V)$ nad K (definirana v A.2.14).

Primer. Dimenzija $\mathbb{A}^n$ je n, saj je $\overline{K}(\mathbb{A}^n) = \overline{K}(x_1, \ldots, x_n)$. Podobno velja, če je $V \subset \mathbb{A}^n$ generirana kot množica ničel enega samega nekonstantnega polinoma. $f(x_1, \ldots, x_n) = 0$. Potem je $\dim(V) = n - 1$, kajti $K[V] = K[x1, \ldots, x_n]/\langle f \rangle$. •

Definicija 3.1.5. Naj bo $V \subset \mathbb{A}^n$, $P \in V$ in $f_1, \ldots, f_m \in \overline{K}[X]$ množica generatorjev $I(V)$. V je **nesingularna** ali **gladka v točki** P, če je rang $m \times n$ matrike

$$(\partial f_i/\partial x_j(P))_{1\leq i\leq m, 1\leq j\leq n}$$

enak $n - \dim(V)$. Če je V nesingularna v vseh točkah, potem pravimo V nesingularna ali gladka raznoterost.

Izberimo točko $P \in V$ in definirajmo ideal v $\overline{K}[V]$ s predpisom

$$M_P = \{f \in \overline{K}[V] : \ f(P) = 0\}.$$

M_P je maksimalni ideal, v posebnem obstaja izomorfizem

$$\begin{array}{ccc} \overline{K}[V]/M_P & \to & \overline{K}, \\ f & \mapsto & f(P). \end{array}$$

Definicija 3.1.6. Lokalni kolobar raznoterosti V v točki P, označen s $\overline{K}[V]_P$, je lokalizacija $\overline{K}[V]$ glede na M_P definirana kot

$$\overline{K}[V]_P = \left\{ \frac{f}{g} \in \overline{K}(V) : \ f, g \in \overline{K}[V], \ g(P) \neq 0 \right\}.$$

Če je $F = f/g \in \overline{K}[V]_P$, potem je $F(P) = f(P)/g(P)$ dobro definirana oziroma regularna v P.

V algebraični geometriji afine raznoterosti naravno vložimo v projektivni prostor. V nadaljevanju bomo definirali še projektivne raznoterosti.

Definicija 3.1.7. Projektivni n-prostor nad obsegom K označen s $\mathbb{P}^n$ ali $\mathbb{P}^n(\overline{K})$ je množica ekvivalenčnih razredov $(n+1)$-teric

$$(x_0, x_1, \ldots, x_n) \in \mathbb{A}^{n+1} - \{0^{n+1}\}$$

glede na ekvivalenčno relacijo

$$(x_0, x_1, \ldots, x_n) \sim \lambda(x_0, x_1, \ldots, x_n)$$

za neničelne $\lambda \in \overline{K}$. Ekvivalenčni razred $\{(\lambda x_0, \ldots, \lambda x_n)\}$ označimo z $X = [x_0, x_1, \ldots, x_n]$ in ga imenujemo **točka** v $\mathbb{P}^n$. Koordinate x_i imenujemo **homogene koordinate** točke X. Množica K-**racionalnih točk** v $\mathbb{P}^n$ je množica

$$\mathbb{P}^n(K) = \{[x_0, \ldots, x_n] \in \mathbb{P}^n : \ \forall x_i \in K\}.$$

Definicija 3.1.8. Polinom $f \in \overline{K}[X]$ je **homogen** stopnje d, če $f(\lambda x_0, \ldots, \lambda x_n) = \lambda^d f(x_0, \ldots, x_n)$, za vsak $\lambda \in \overline{K}$. Ideal $I \subset \overline{K}[X]$ je homogen, če je generiran s homogenimi polinomi.

Definicija 3.1.9. Projektivna algebraična množica homogenega ideala I je množica oblike

$$V_I = \{P \in \mathbb{P}^n : \ f(P) = 0, \ \forall \text{ homogen } f \in I\}.$$

Če je V projektivna algebraična množica, je **homogeni ideal** množice V definiran kot

$$I(V) = \{f \in \overline{K}[X] : \ f \text{ homogen in } f(P) = 0, \ \forall P \in V\}.$$

Projektivna algebraična množica V je **definirana nad** K, če je njen ideal $I(V)$ generiran s homogenimi polinomi v $K[X]$, kar označimo z V/K. Množica K-racionalnih točk množice V/K je naslednja množica:

$$V(K) = V \cap \mathbb{P}^n(K).$$

Definicija 3.1.10. Projektivna algebraična množica je **projektivna raznoterost**, če je pripadajoči homogeni ideal $I(V)$ praideal v $\overline{K}[X]$.

V nadaljevanju si oglejmo preslikavi

$$\begin{array}{rccc} \phi_i : & \mathbb{A}^n & \to & \mathbb{P}^n, \\ & (y_1, \ldots, y_n) & \mapsto & [y_1, \ldots, y_{i-1}, 1, y_i, \ldots, y_n] \end{array}$$

in

$$\begin{array}{rccc} \phi_i^{-1} : & U_i & \to & \mathbb{A}_i^n, \\ & [x_0, \ldots, x_n] & \mapsto & (\frac{x_0}{x_i}, \ldots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \ldots, \frac{x_n}{x_i}), \end{array}$$

kjer je $U_i = \{[x_0, \ldots, x_n] \in \mathbb{P}^n : \ x_i \neq 0\}$.
Procesu zamenjave $f(x_0, \ldots, x_n)$ z $f(y_1, \ldots, y_{i-1}, 1, y_i, \ldots, y_n)$ pravimo **dehomogenizacija** glede na x_i. Proces lahko tudi obrnemo. Za polinom f v n spremenljivkah nad $\overline{K}$ naj bo

$$f^*(x_0, \ldots, x_n) = x_i^d f\left(\frac{x_0}{x_i}, \ldots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \ldots, \frac{x_n}{x_i}\right),$$

kjer je $d = \deg(f)$ najmanjše celo število za katerega je f^* polinom. Pravimo, da je f^* **homogenizacija** f glede na x_i.

Definicija 3.1.11. Naj bo V afina algebraična množica z idealom $I(V)$. **Projektivno zaprtje** množice V glede na vložitev $V \subset \mathbb{A}^n \xrightarrow{\phi_i} \mathbb{P}^n$ je projektivna algebraična množica $\overline{V} \subset \mathbb{P}^n$, katere homogeni ideal je generiran z

$$\{f^* : \ f \in I(V)\}.$$

Trditev 3.1.12. *[137, Trditev I.2.6].*

1. *Naj bo V afina raznoterost. Potem je $\overline{V}$ projektivna raznoterost in $V = \overline{V} \cap \mathbb{A}^n$.*
2. *Naj bo V projektivna raznoterost. Potem je $V \cap \mathbb{A}^n$ afina raznoterost in velja*

$$V \cap \mathbb{A}^n = \emptyset \quad ali \quad V = \overline{V \cap \mathbb{A}^n}.$$

3. *Če je afina (projektivna) raznoterost V definirana nad K, potem je $\overline{V}$ (respektivno $V \cap \mathbb{A}^n$) prav tako definirana nad K.*

■

Primer. Naj bo $V \subset \mathbb{A}^n$ afina raznoterost dana z enačbo $Y^2 = X^3 + 17$. Enačbo homogeniziramo s substitucijo $X = \overline{X}/\overline{Z}$, $Y = \overline{Y}/\overline{Z}$ in dobimo projektivno raznoterost v $\mathbb{P}^2$ s homogeno enačbo $\overline{Y}^2\overline{Z} = \overline{X}^3 + 17\overline{Z}^3$. Projektivna raznoterost ima dodatno točko $[0, 1, 0]$ v neskončnosti, ki jo dobimo tako, da postavimo $\overline{Z} = 0$. Od tod sklepamo,

$$V(\mathbb{Q}) = \{[x, y, 1] \in \mathbb{P}^2(\mathbb{Q}) : \ y^2 = x^3 + 17\} \cup \{[0, 1, 0]\}.$$

•

Večino lastnosti projektivne raznoterosti V lahko definiramo v jeziku afinih raznoterosti $V \cap \mathbb{A}^n$.

Definicija 3.1.13. Za projektivno raznoterost V/K izberimo afin prostor $\mathbb{A}^n \subset \mathbb{P}^n$, da $V \cap \mathbb{A}^n \neq \emptyset$. **Dimenzija** V je dimenzija $V \cap \mathbb{A}^n$. **Lokalni kolobar** V v točki $P = [p_0, p_1, \ldots, p_n] \in \mathbb{P}^n$, označen kot $\overline{K}[V]_P$, je lokalni kolobar $V \cap \mathbb{A}^n$ v točki $P = \left(\frac{p_0}{p_i}, \frac{p_1}{p_i}, \ldots, \frac{p_n}{p_i}\right) \in \mathbb{A}^n$. Funkcija $F \in \overline{K}(V)$ je **regularna** oziroma **definirana v** P, če je element $\overline{K}[V]_P$.

Analogno s pomočjo dehomogenizacije podamo tudi **obseg racionalnih funkcij** $K(V)$ in $\overline{K}(V)$. Obseg racionalnih funkcij na $\mathbb{P}^n$ lahko opišemo tudi kot podobseg $\overline{K}(x_0, \ldots, x_n)$, ki je sestavljen iz racionalnih funkcij $F = f/g$, kjer sta f in g homogena polinoma enakih stopenj. Tak opis porodi dobro definirane funkcije na $\mathbb{P}^n$ za vse točke P, za katere je $g(P) \neq 0$. Podobno obseg racionalnih funkcij projektivne raznoterosti sestavljajo take racionalne funkcije $F = f/g$, da velja:

- f in g sta homogena in enake stopnje;
- $g \notin I(V)$;
- funkciji f/g in f'/g' sta identični, če je $fg' - f'g \in I(V)$.

Zdaj ko smo podali osnovne definicije afinih in projektivnih raznoterosti, si lahko ogledamo preslikave med raznoterostmi.

Definicija 3.1.14. Naj bosta $V_1, V_2 \subset \mathbb{P}^n$ projektivni raznoterosti. **Racionalna preslikava** je podana z $(n+1)$-terico racionalnih funkcij $f_0, f_1, \ldots, f_n \in \overline{K}(V_1)$ po naslednjem predpisu

$$\begin{array}{rccc} \phi: & V_1 & \to & V_2, \\ & P & \mapsto & [f_0(P), f_1(P), \ldots, f_n(P)]. \end{array}$$

Definicijsko območje ϕ sestavljajo točke $P \in V_1$ v katerih so definirane vse f_i. Če obstaja tak neničelni $\lambda \in \overline{K}$, da so $\lambda f_0, \ldots, \lambda f_n \in K(V_1)$, potem pravimo, da je ϕ **definirana nad** K.

Definicija 3.1.15. Racionalna preslikava $\phi = [f_0, \ldots, f_n] : V_1 \to V_2$ je **regularna** oziroma **definirana v točki** $P \in V_1$, če obstaja taka funkcija $g \in \overline{K}(V_1)$, da velja:

1. gf_i je regularna v točki P za vsak $i = 0, 1, \ldots, n$;
2. za nek i je $(gf_i)(P) \neq 0$.

Če taka funkcija g obstaja, potem je očitno

$$\phi(P) = [(gf_0)(P), \ldots, (gf_n)(P)].$$

Racionalna preslikava, ki je regularna v vsaki točki $P \in V_1$, se imenuje **morfizem**.

Definicija 3.1.16. Raznoterosti V_1 in V_2 sta **izomorfni** $V_1 \simeq V_2$, če obstajata morfizma $\phi : V_1 \to V_2$ in $\psi : V_2 \to V_1$, za katera velja $\psi \circ \phi = \mathrm{id}_{V_1}$ in $\phi \circ \psi = \mathrm{id}_{V_2}$. V_1/K in V_2/K sta izomorfni nad K, če sta zgornja ϕ in ψ definirani nad K.

Če je $\phi : V_1 \to V_2$ izomorfizem definiran nad K, potem ϕ identificira $V_1(K)$ z $V_2(K)$. Pri Diofantskih problemih je zato dovolj, če izberemo enega predstavnika v razredu K-izomorfnih raznoterosti.

3.2 Algebraične krivulje

V tem razdelku si bomo ogledali definicijo in lastnosti algebraičnih krivulj, ki veljajo seveda tudi za eliptične krivulje. **Algebraična krivulja** je projektivna algebraična raznoterost dimenzije 1.

Uporabljali bomo naslednje oznake:

- C je krivulja in $P \in C$ je točka na krivulji;
- C/K je krivulja C definirana nad obsegom K;
- $K(C)$ in $\overline{K}(C)$ označujeta obseg racionalnih funkcij krivulje C;
- $\overline{K}[C]_P$ je lokalni kolobar krivulje C v točki P;
- M_P je maksimalni ideal lokalnega kolobarja $\overline{K}[C]_P$.

Trditev 3.2.1. *[137, Trditev II.1.1]. Naj bo C krivulja in $P \in C$ gladka točka. Potem je $\overline{K}[C]_P$ diskretni valuacijski kolobar, definiran v A.4.1.* ■

Definicija 3.2.2. Naj bo P gladka točka na krivulji C. **Normalizirana valuacija** na $\overline{K}[C]_P$ je podana z

$$\begin{array}{rccl} \mathrm{ord}_P : & \overline{K}[C]_P & \to & \{0, 1, 2, \ldots\} \cup \{\infty\} \\ & f & \mapsto & \max\{d \in \mathbb{Z} : \ f \in M_P^d\}. \end{array}$$

S predpisom $\mathrm{ord}_P(f/g) = \mathrm{ord}_P(f) - \mathrm{ord}_P(g)$, lahko ord_P razširimo tudi na $\overline{K}(C)$. **Uniformizator** za C v točki P je funkcija $v \in \overline{K}(C)$ z $\mathrm{ord}_P(v) = 1$; drugače povedano, v je generator ideala M_P.

Definicija 3.2.3. Izberimo gladko točko $P \in C$ in $f \in \overline{K}(C)$. **Red funkcije** f v točki P je $\mathrm{ord}_P(f)$. Če je $\mathrm{ord}_P(f) > 0$, potem ima f v točki P ničlo, če je $\mathrm{ord}_P(f) < 0$, pa ima f v točki P pol. Za $\mathrm{ord}_P(f) \geq 0$ je f regularna in lahko izračunamo $f(P)$, sicer za pol pišemo $f(P) = \infty$.

Trditev 3.2.4. *[137, Trditev II.1.2]. Naj bo C gladka krivulja in $f \in \overline{K}(C)$. Potem je na C kvečjemu končno število točk v katerih ima f pol ali ničlo. Če f nima niti pola, niti ničle, je $f \in \overline{K}$ konstantna.* ■

Naslednja trditev je koristna, za obsege s karakteristiko $p > 0$.

Trditev 3.2.5. *[137, Trditev II.1.4]. Naj bo C/K krivulja in naj bo $v \in K(C)$ uniformizator v neki gladki točki $P \in C$. Potem je $K(C)$ končna separabilna razširitev obsega $K(v)$, definirana v A.2.6.* ■

Za vsak $\sigma \in \mathrm{Gal}_{\overline{K}/K}$ je $\mathrm{ord}_P(f) = \mathrm{ord}_{\sigma(P)}(\sigma(f))$.

3.2.1 Preslikave med krivuljami

Trditev 3.2.6. *Naj bo $\phi : C \to V$ racionalna preslikava med krivuljo C in raznoterostjo $V \subset \mathbb{P}^n$. Potem je preslikava ϕ regularna v gladki točki $P \in C$. Posledično je ϕ morfizem za gladko krivuljo C.*

Dokaz. Naj bo $\phi = [f_0, \ldots, f_N]$, kjer so $f_i \in \overline{K}(C)$. Izberimo uniformizator $v \in \overline{K}(C)$ za krivuljo C v točki P. Naj bo $n = \min_{0 \leq i \leq N}\{\mathrm{ord}_P(f_i)\}$. Potem velja $\mathrm{ord}_P(v^{-n} f_i) \geq 0$ za vsak i in $\mathrm{ord}_P(v^{-n} f_j) = 0$ za nek j, torej so vsi $v^{-n} f_i$ regularni v P in $(v^{-n} f_j)(P) \neq 0$. ■

Naj bo C/K gladka krivulja in $f \in K(C)$ funkcija. Z f lahko definiramo racionalno preslikavo

$$\begin{array}{rccc} \ell : & C & \to & \mathbb{P}^1 \\ & P & \mapsto & [f(P), 1]. \end{array}$$

Ta preslikava je dejansko morfizem, ki po točkah deluje z naslednjim pravilom:

$$\ell(P) = \begin{cases} [f(P), 1] & ; \text{če je f regularna v P,} \\ [1, 0] & ; \text{če ima f pol v točki P.} \end{cases} \tag{3.3}$$

Naj bo zdaj $\phi : C \to \mathbb{P}^1$, $\phi = [f, g]$ racionalna preslikava definirana nad K. V primeru da je $g = 0$, je $\phi = [1, 0]$ konstantna preslikava, sicer pa je $\phi = [f/g, 1]$ preslikava, ki ustreza $f/g \in K(C)$. Konstantno preslikavo $\phi = [1, 0]$ označimo z ∞ in dobimo korespondenco

$$K(C) \cup \{\infty\} \leftrightarrow \{\text{preslikave } C \to \mathbb{P}^1 \text{ definirane nad } K\}.$$

Izrek 3.2.7. *[137, Izrek II.2.3]. Naj bo $\phi : C_1 \to C_2$ morfizem krivulj. Potem je ϕ ali konstantna ali surjektivna.* ■

Naj bosta C_1/K in C_2/K krivulji in $\phi : C_1 \to C_2$ nekonstantna racionalna preslikava definirana nad K. Komponiranje s ϕ porodi injektivno preslikavo med obsegoma racionalnih funkcij, ki fiksira obseg K :

$$\begin{array}{rccc} \phi^* : & K(C_2) & \to & K(C_1) \\ & f & \mapsto & f \circ \phi. \end{array} \tag{3.4}$$

Izrek 3.2.8. *[137, Izrek II.2.4]. Za krivulji C_1/K in C_2/K veljajo naslednje trditve:*

1. *Naj bo $\phi : C_1 \to C_2$ nekonstantna racionalna preslikava definirana nad K. Potem je $K(C_1)$ končna razširitev $\phi^* K(C_2)$.*
2. *Naj bo $\ell : K(C_2) \to K(C_1)$ injektivna preslikava med obsegoma funkcij, ki fiksira K. Potem obstaja enolična nekonstantna racionalna preslikava $\phi : C_1 \to C_2$ definirana nad K, za katero velja $\phi^* = \ell$.*
3. *Naj bo $\mathbb{K} \subset K(C_1)$ podobseg končnega indeksa, ki vsebuje K. Potem obstajata gladka krivulja C'/K, enolično določena do K-izomorfizma natančno, in nekonstantna racionalna preslikava $\phi : C_1 \to C'$ definirana nad K, tako da velja $\phi^* K(C') = \mathbb{K}$.*

■

Definicija 3.2.9. Kot običajno naj bo $\phi : C_1 \to C_2$ racionalna preslikava definirana nad K. **Stopnjo** ϕ definiramo kot

$$\deg \phi = \begin{cases} 0 & ; \text{če je } \phi \text{ konstantna,} \\ [K(C_1) : \phi^* K(C_2)] & ; \text{če } \phi \text{ ni konstantna.} \end{cases} \tag{3.5}$$

Pravimo, da je ϕ **separabilna (neseparabilna, čisto neseparabilna)**, če ima dotično lastnost razširitev $K(C_1)/\phi^* K(C_2)$. Separabilno in neseparabilno stopnjo označimo zaporedoma z $\deg_s \phi$ in $\deg_i \phi$.

Definicija 3.2.10. Naj bo $\phi : C_1 \to C_2$ nekonstantna racionalna preslikava definirana nad K. S pomočjo norme (definirane v A.2.16) glede na ϕ^* definiramo $\phi_* : K(C_1) \to K(C_2)$ kot

$$\phi_* = (\phi^*)^{-1} \circ N_{K(C_1)/\phi^* K(C_2)}.$$

Trditev 3.2.11. *Naj bosta C_1 in C_2 gladki krivulji in naj bo $\phi : C_1 \to C_2$ stopnje 1. Potem je ϕ izomorfizem.*

Dokaz. Po definiciji stopnje $\deg \phi = 1$ pomeni, da je $\phi^* \overline{K}(C_2) = \overline{K}(C_1)$, torej je ϕ^* izomorfizem obsega funkcij. Po točki 2. izreka 3.2.8 za inverzno preslikavo $(\phi^*)^{-1} : \overline{K}(C_1) \to \overline{K}(C_2)$ obstaja taka racionalna preslikava $\psi : C_2 \to C_1$, da je $\psi^* = (\phi^*)^{-1}$. Ker je C_2 gladka, je ψ dejansko morfizem. Iz $(\phi \circ \psi)^* = \psi^* \circ \phi^* = \mathrm{id}_{\overline{K}(C_2)}$ in $(\psi \circ \phi)^* = \phi^* \circ \psi^* = \mathrm{id}_{\overline{K}(C_1)}$ zaradi enoličnosti v točki 2. izreka 3.2.8 sledi, da sta $\phi \circ \psi = \mathrm{id}_{C_2}$ in $\psi \circ \phi = \mathrm{id}_{C_1}$ Torej sta ϕ in ψ izomorfizma. ■

Izrek 3.2.8 in trditev 3.2.11 povežeta krivulje s pripadajočimi obsegi racionalnih funkcij v smislu ekvivalence kategorij [137, poglavje II.2].

Definicija 3.2.12. Naj bo $\phi : C_1 \to C_2$ nekonstantna racionalna preslikava gladkih krivulj. Za izbrano točko $P \in C_1$ je **indeks ramifikacije** ϕ definiran kot

$$e_\phi(P) = \mathrm{ord}_P(\phi^* t_{\phi(P)}),$$

kjer je $t_{\phi(P)} \in K(C_2)$ uniformizator v točki $\phi(P)$. Ker vedno velja $e_\phi(P) \geq 1$, pravimo, da je ϕ **neramificirana v točki** P za $e_\phi(P) = 1$. Če je ϕ neramificirana v vseh točkah, rečemo da je **neramificirana**.

Trditev 3.2.13. *[137, Trditev II.2.6] Za nekonstantno racionalno preslikavo $\phi : C_1 \to C_2$ med gladkima krivuljama veljajo naslednje trditve:*

1. *Za vsako točko $Q \in C_2$ je*

$$\sum_{P \in \phi^{-1}(Q)} e_\phi(P) = \deg \phi;$$

2. *Za vse razen za končno mnogo točk $Q \in C_2$ velja*

$$\#\phi^{-1}(Q) = \deg_s(\phi);$$

3. *Naj bo $\psi : C_2 \to C_3$ nekonstantna racionalna preslikava med gladkima krivuljama. Za vsak $P \in C_1$ velja*

$$e_{\psi\circ\phi}(P) = e_\phi(P) e_\psi(\phi(P)).$$

■

Posledica 3.2.14. *Preslikava $\phi : C_1 \to C_2$ je neramificirana natanko tedaj, ko je $\#\phi^{-1}(Q) = \deg(\phi)$ za vsak $Q \in C_2$.*

Dokaz. Iz točke 1. trditve 3.2.13 sledi, da je $\#\phi^{-1}(Q) = \deg \phi$ ekvivalentno

$$\sum_{P \in \phi^{-1}(Q)} e_\phi(P) = \#\phi^{-1}(Q).$$

Ker je $e_\phi(P) \geq 1$ je to res natanko tedaj, ko je $e_\phi(P) = 1$. ■

Opomnimo, da je trditev 3.2.13 analogna izrekom, ki opisujejo ramifikacijo praštevil v številskih obsegih. Za številski obseg L/K je postavka 1. analogna dejstvu $\sum e_i f_i = [K : \mathbb{Q}]$; postavka 2. je analogna dejstvu, da samo končno mnogo praštevil obsega K ramificira v obsegu L; postavka 3. pa nam da večkratnost stopnje ramifikacije v stolpu obsegov [86].

Primer. Naj bo $\phi : \mathbb{P}^1 \to \mathbb{P}^1$ preslikava med premicama dana s predpisom $\phi([X, Y]) = [X^3(X - Y)^2, Y^5]$. Preslikava ϕ je ramificirana v točkah $[0, 1]$ in $[1, 1]$. Velja $e_\phi([0, 1]) = 3$ in $e_\phi([1, 1]) = 2$, posledično je

$$\sum_{P \in \phi^{-1}([0,1])} e_\phi(P) = e_\phi([0, 1]) + e_\phi([1, 1]) = 5 = \deg \phi.$$

•

3.2.2 Frobeniusova preslikava

Dan je obseg K s karakteristiko $p > 0$ in število oblike $q = p^r$. Polinomu $f \in K[X]$ priredimo polinom $f^{(q)}$, tako da vsak koeficient dvignemo na q-to potenco. Potem za poljubno krivuljo C/K lahko definiramo novo krivuljo $C^{(q)}/K$, tako da opišemo njen homogen ideal kot

$$I(C^{(q)}) = \langle \{ f^{(q)} : \ f \in I(C) \rangle.$$

Definicija 3.2.15. Frobeniusov morfizem je preslikava

$$\begin{array}{rccc} \phi : & C & \to & C^{(q)}, \\ & [x_0, \ldots, x_n] & \mapsto & [x_0^q, \ldots, x_n^q]. \end{array}$$

Za dobro definiranost ϕ je dovolj dokazati, da je za vsak $P = [x_0, \ldots, x_n] \in C$ slika $\phi(P) \in C^{(q)}$. Res, $\phi(P)$ je ničla vsakega generatorja $f^{(q)}$ ideala $I(C^{(q)})$:

$$\begin{array}{rcll} f^{(q)}(\phi(P)) & = & f^{(q)}(x_0^q, \ldots, x_n^q) & \\ & = & (f(x_0, \ldots, x_n))^q & \text{ker je } \mathrm{char}(K) = p \\ & = & 0 & \text{ker je } f(P) = 0. \end{array}$$

Primer. Naj bo C krivulja v $\mathbb{P}^2$ podana z enačbo

$$Y^2Z = X^3 + aX^2Z + bZ^3.$$

Krivulja $C^{(q)}$ ima potem enačbo

$$Y^2Z = X^3 + a^qX^2Z + b^qZ^3.$$

•

V naslednji trditvi bomo opisali osnovne lastnosti Frobeniuosove preslikave.

Trditev 3.2.16. *[137, Trditev II.2.11]. Naj bo K popolni obseg karakteristike $p > 0$ (definiran v A.2.8). Za krivuljo C nad K in Frobeniusov morfizem $\phi : C \to C^{(q)}$ veljajo naslednje trditve:*

1. $\phi^* K(C^{(q)}) = K(C)^q = \{ f^q : \ f \in K(C) \}$, *kjer je ϕ^* definiran v* (3.4)*;*
2. *ϕ je čisto neseparabilen;*
3. $\deg \phi = q$.

■

Posledica 3.2.17. *[137, Posledica II.2.12]. Vsaka preslikava $\psi : C_1 \to C_2$ gladkih krivulj nad obsegom karakteristike $p > 0$ faktorizira kot*

$$C_1 \overset{\phi}{\to} C_1^{(q)} \overset{\lambda}{\to} C_2,$$

kjer je $q = \deg_i(\psi)$, ϕ je q-ti Frobeniusov morfizem in λ je separabilna. ■

3.3 Delitelji

Delitelji so sestavljeni iz podraznoterosti kodimenzije 1. Iz grupe deliteljev lahko razberemo veliko informacij o raznoterostih. Med drugim z delitelji definiramo grupo na eliptični krivulji, uporabljajo pa se tudi pri računanju parjenj, zato si jih bomo v nadaljevanju podrobneje ogledali. Podobno kot v prejšnjih razdelkih, bomo tudi delitelje vpeljali na projektivnih krivuljah, tj. algebraičnih raznoterostih dimenzije 1. V nadaljevanju bo C označevala krivuljo definirano nad obsegom K. Kot vedno bomo računali s točkami nad $\overline{K}$.

Definicija 3.3.1. Delitelj D je formalna vsota točk

$$D = \sum_{P \in C} n_P(P), \tag{3.6}$$

kjer $n_P \in \mathbb{Z}$ in $n_P = 0$ za vse razen za končno mnogo točk $P \in C$. Delitelj, kjer so vsi $n_P = 0$, označimo z 0. **Podpora** delitelja je končna množica

$$\mathrm{Supp}(D) = \{P \in C : \ n_P \neq 0\}.$$

Definirajmo še

$$-D = \sum_{P \in C} (-n_P)(P),$$

in vsoto

$$D + D' = \sum_{P \in C} (n_P + n'_P)(P).$$

Če je $D = \sum_{i=1}^{m} n_m(P)$, kjer so vsi $n_m \geq 0$, potem označimo $D \geq 0$ in ga imenujemo **učinkoviti delitelj**. Relacijo $\geq$ definiramo s pravilom

$$D \geq D' \Leftrightarrow n_P \geq n'_P \ \forall P \in C.$$

Množico vseh deliteljev krivulje C označimo z $\mathrm{Div}(C)$.

Trditev 3.3.2. *Množica vseh deliteljev* $\mathrm{Div}(C)$ *na krivulji* C *je prosta Abelova grupa.* ■

Definicija 3.3.3. Stopnja delitelja D je definirana z

$$\deg D = \sum_{P \in C} n_P. \tag{3.7}$$

Z

$$\mathrm{Div}^0(C) = \{D \in \mathrm{Div}(C) : \ \deg D = 0\}$$

označimo množico deliteljev stopnje 0.

Lema 3.3.4. $\mathrm{Div}^0(C)$ *je podgrupa grupe* $\mathrm{Div}(C)$. ■

Definicija 3.3.5. Naj bo $D = \sum_{P \in C} n_P(P)$ delitelj na krivulji C. Za $\sigma \in \mathrm{Gal}(\overline{K}/K)$ definiramo $\sigma(D) = \sum_{P \in C} n_P(\sigma(P))$. Pravimo, da je D **definiran nad obsegom** K, če je $\sigma(D) = D$ za vsak $\sigma \in \mathrm{Gal}(\overline{K}/K)$. Grupo deliteljev definiranih nad K označimo z $\mathrm{Div}_K(C)$ in podgrupo deliteljev reda 0 označimo z $\mathrm{Div}^0_K(C)$.

Če je delitelj $D = n_1(P_1) + \ldots + n_m(P_m)$ definiran nad K, to ne implicira nujno, da so vsi $P_i \in C(K)$.

Primer. Naj bo $C: \ x^2+y^2 = 6z^2$ definirana nad $\mathbb{Q}$ in naj bosta $P = [1+\sqrt{2}, 1-\sqrt{2}, 1]$, $Q = [1-\sqrt{2}, 1+\sqrt{2}, 1] \in C(\mathbb{Q}(\sqrt{2})) \subset C(\overline{K})$. Izberimo $D = (P)+(Q)$. Dovolj je preveriti $\sigma(D)$ za vsak $\sigma \in \mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$. Edini netrivialni avtomorfizem je $\sigma(\sqrt{2}) = -\sqrt{2}$, zato je $\sigma(P) = Q$ in $\sigma(Q) = P$. Torej velja $\sigma(D) = D$ in D je definiran nad $\mathbb{Q}$. •

Definicija 3.3.6. Naj bo C gladka krivulja in naj bo $f \in \overline{K}(C)^*$. **Delitelj funkcije** f je definiran kot

$$\mathrm{div}(f) = \sum_{P \in C} \mathrm{ord}_P(f)(P).$$

Delitelj $D \in \mathrm{Div}(C)$ je **glavni delitelj**, če je oblike $D = \mathrm{div}(f)$ za neko funkcijo $f \in \overline{K}(C)^*$. Množico glavnih deliteljev označimo s $\mathrm{Prin}(C)$.

Red funkcije $\mathrm{ord}_P(f)$ smo definirali v 3.2.2. Po trditvi 3.2.4 je zgoraj definiran $\mathrm{div}(f)$ res delitelj. Lastnosti glavnih deliteljev so zajete v naslednji trditvi.

Trditev 3.3.7. *Za racionalni funkciji $f, f' \in \overline{K}(C)^*$ na gladki krivulji C veljajo naslednje trditve:*

1. $\mathrm{div}(ff') = \mathrm{div}(f) + \mathrm{div}(f')$;
2. $\mathrm{div}(1/f) = -\mathrm{div}(f)$;
3. $\mathrm{div}(f+f') \geq \sum_{P \in C} \min\{\mathrm{ord}(f), \mathrm{ord}(f')\}(P)$;
4. $\mathrm{div}(f^n) = n \cdot \mathrm{div}(f)$, *za poljuben* $n \in \mathbb{Z}$;
5. *Naj bo* $f \in \overline{K}(C)$ *in* $\sigma \in \mathrm{Gal}_{\overline{K}/K}$, *potem je* $\mathrm{div}(\sigma(f)) = \sigma(\mathrm{div}(f))$;
6. *Če je* $f \in K(C)$, *potem je* $\mathrm{div}(f) \in \mathrm{Div}_K(C)$;
7. *Preslikava* $\mathrm{div}: \overline{K}(C)^* \to \mathrm{Div}(C)$ *je homomorfizem Abelovih grup;*
8. $\mathrm{Prin}(C)$ *je podgrupa grupe* $\mathrm{Div}(C)$.

Dokaz.

1. $$\begin{aligned} \mathrm{div}(ff') &= \textstyle\sum_P \mathrm{ord}_P(ff')(P) \\ &= \textstyle\sum_P (\mathrm{ord}_P(f) + \mathrm{ord}_P(f'))(P) \\ &= \textstyle\sum_P \mathrm{ord}_P(f)(P) + \sum_P \mathrm{ord}_P(f')(P) \\ &= \mathrm{div}(f) + \mathrm{div}(f'). \end{aligned}$$

2. Po definiciji 3.2.2 izračunamo $\mathrm{ord}_P(1/f) = \mathrm{ord}_P(1) - \mathrm{ord}_P(f) = -\mathrm{ord}_P(f)$. Sledi, $\mathrm{div}(1/f) = -\mathrm{div}(f)$.

3. Sledi iz definicije $\mathrm{div}(f)$ in dejstva, da je $\mathrm{ord}_P(f+f') \geq \min\{\mathrm{ord}(f), \mathrm{ord}(f')\}$.

4. V točki 1. izberimo $f = f'$ in uporabimo indukcijo.

5.
$$\begin{aligned}\operatorname{div}(\sigma(f)) &= \textstyle\sum_P \operatorname{ord}(\sigma(f))(P) \\ &= \textstyle\sum_P \operatorname{ord}(\sigma(f))(\sigma(P)) && \text{sledi iz enakost 3.2 na strani 14} \\ &= \textstyle\sum_P \operatorname{ord}(f)(\sigma(P)) && \text{sledi iz lastnosti ord na strani 19} \\ &= \sigma(\operatorname{div}(f)).\end{aligned}$$

6. Za $f \in K(C)$ po enakosti (3.1) velja $\sigma(f) = f$. Iz točke 5. in definicije 3.3.5 potem sledi $\operatorname{div}(f) \in \operatorname{Div}_K(C)$.

7. Sledi iz definicije glavnih deliteljev in dejstva, da je ord_P diskretna valuacija na obsegu racionalnih funkcij. Definicijo valuacije najdemo v dodatku A.4.

8. Sledi iz prejšnjih točk.

■

Definicija 3.3.8. Delitelja D_1 in D_2 sta **linearno ekvivalentna** $D_1 \sim D_2$ če je $D_1 - D_2$ glavni delitelj. **Grupa razredov deliteljev** (ang. divisor class group) krivulje C ali **Picardova grupa** krivulje C označena s $\operatorname{Pic}(C)$ je faktorska grupa $\operatorname{Div}(C)/\operatorname{Prin}(C)$. S $\operatorname{Pic}_K(C)$ označimo podgrupo deliteljev $\operatorname{Pic}(C)$, ki jih $\operatorname{Gal}_{\overline{K}/K}$ pusti fiksirane.

V splošnem ne velja, da je $\operatorname{Pic}_K(C)$ faktorska grupa $\operatorname{Div}_K(C)$ po njeni podgrupi glavnih deliteljev.

Lema 3.3.9. *Na premici $\mathbb{P}^1$ je vsak delitelj stopnje 0 glavni delitelj. Preslikava*

$$\deg : \operatorname{Pic}(\mathbb{P}^1) \to \mathbb{Z}$$

je izomorfizem.

Dokaz. Naj ima delitelj $D = \sum_P n_P(P)$ stopnjo 0. Označimo $P = [\alpha_P, \beta_P]$. Vidimo, da je D delitelj racionalne funkcije

$$\prod_{P \in \mathbb{P}^1} (\beta_P X - \alpha_P Y)^{n_P}.$$

Ta funkcija je v $K(\mathbb{P}^1)$, saj je $\sum n_P = 0$. Nevtralni element grupe $\operatorname{Pic}(\mathbb{P}^1)$ je ekvivalenčni razred glavnih deliteljev in ker so vsi delitelji stopnje 0 glavni, je preslikava injektivna. Surjektivnost sledi iz dejstva, da je deg diskretna valuacija (katere opis je v dodatku A.4.5). ■

V [137, poglavje II] najdemo tudi obrat; če je C gladka krivulja s Picardovo grupo $\operatorname{Pic}(C) \simeq \mathbb{Z}$, potem je C izomorfna $\mathbb{P}^1$.

Izrek 3.3.10. *Naj bo C gladka krivulja in $f \in \overline{K}(C)^*$. Potem je* $\operatorname{div}(f) = 0$ *natanko tedaj, ko je $f \in \overline{K}^*$.*

Dokaz. Če je $\operatorname{div}(f) = 0$, potem f nima polov in zato porojena preslikava $\ell : C \to \mathbb{P}^1$ (3.3) na strani 19 ni surjektivna. Po izreku 3.2.7 je taka preslikava konstantna, torej je $f \in \overline{K}^*$. ■

Primer. Naj bo $\mathrm{char}(K) \neq 0$ in naj bodo $e_1, e_2, e_3 \in \overline{K}$ različni. Oglejmo si krivuljo z naslednjo enačbo:

$$C: \ y^2 z = (x - e_1 z)(x - e_2 z)(x - e_3 z).$$

Krivulja je gladka in ima točko $[0, 1, 0]$ v neskončnosti, ki jo bomo označili s P_∞. Naj bodo $P_i = [e_i, 0, 1] \in C$ za $i = 1, 2, 3$. Potem lahko izračunamo

$$\mathrm{div}\left(\frac{x - e_i z}{z}\right) = 2(P_i) + (P_\infty) - 3(P_\infty) = 2(P_i) - 2(P_\infty)$$

in

$$\mathrm{div}\left(\frac{y}{z}\right) = (P_1) + (P_2) + (P_3) - 3(P_\infty).$$

•

Definicija 3.3.11. V Picardovi grupi $\mathrm{Pic}(C)$ označimo delitelje s stopnjo 0 s $\mathrm{Pic}^0(C)$. To je faktorska grupa grupe $\mathrm{Div}^0(C)$ z njeno podgrupo glavnih deliteljev. Definirajmo še $\mathrm{Pic}^0_K(C)$ kot podgrupo $\mathrm{Pic}^0(C)$, fiksirano z $\mathrm{Gal}_{\overline{K}/K}$.

Opomba: Izrek 3.3.10 in definicijo 3.3.11 lahko povzamemo z naslednjim eksaktnim zaporedjem

$$1 \to \overline{K}^* \to \overline{K}(C)^* \xrightarrow{\mathrm{div}} \mathrm{Div}^0(C) \to \mathrm{Pic}^0(C) \to 0. \tag{3.8}$$

Naj bo $\phi : C_1 \to C_2$ nekonstantna racionalna preslikava med gladkimi krivuljami. Kot smo videli v razdelku 3.2.1, ϕ porodi preslikavi na obsegu racionalnih funkcij

$$\phi^* : \overline{K}(C_2) \to \overline{K}(C_1) \ \text{ in } \ \phi_* : \overline{K}(C_1) \to \overline{K}(C_2).$$

Podobno definiramo preslikave na grupi deliteljev in sicer:

$$\begin{array}{rccc} \phi^*: & \mathrm{Div}(C_2) & \to & \mathrm{Div}(C_1) \\ & (Q) & \mapsto & \displaystyle\sum_{P \in \phi^{-1}(Q)} e_\phi(P)(P) \end{array} \quad \text{in} \quad \begin{array}{rccc} \phi_*: & \mathrm{Div}(C_1) & \to & \mathrm{Div}(C_2) \\ & (P) & \mapsto & (\phi(P)). \end{array} \tag{3.9}$$

Za dani delitelj $D = \sum_{P \in C} n_p(P) \in \mathrm{Div}(C)$ izberimo tako racionalno funkcijo $f \in \overline{K}(C)^*$, da sta podpori deliteljev D in $\mathrm{div}(f)$ disjunktni. Potem lahko definiramo

$$f(D) = \prod_{P \in C} f(P)^{n_p}. \tag{3.10}$$

Trditev 3.3.12. *Za nekonstantno preslikavo $\phi : C_1 \to C_2$ med gladkima krivuljama velja:*

1. $\deg(\phi^* D) = (\deg \phi)(\deg D)$ *za vsak* $D \in \mathrm{Div}(C_2)$;
2. $\phi^*(\mathrm{div}\ f) = \mathrm{div}(\phi^* f)$ *za vsak* $f \in \overline{K}(C_2)^*$;
3. $\deg(\phi_* D) = \deg D$ *za vsak* $D \in \mathrm{Div}(C_1)$;
4. $\phi_*(\mathrm{div}\ f) = \mathrm{div}(\phi_* f)$ *za vsak* $f \in \overline{K}(C_1)^*$;
5. $\phi_* \circ \phi^*$ *deluje kot množenje z* $\deg \phi$ *na* $\mathrm{Div}(C_2)$;

6. *Naj bo C_3 gladka krivulja in $\psi : C_2 \to C_3$ nekonstantna preslikava. Potem velja $(\psi \circ \phi)^* = \phi^* \circ \psi^*$ in $(\psi \circ \phi)_* = \psi_* \circ \phi_*$;*

7. *Izberimo take $f_1 \in K(C_1)^*$ in $f_2 \in K(C_2)^*$, ter $D_1 \in \mathrm{Div}(C_1)$ in $D_2 \in \mathrm{Div}(C_2)$, da sta podpori $\mathrm{div}(f_1)$ in $\mathrm{div}(f_2)$ zaporedoma disjunktni od podpor D_1 in D_2. Potem velja:*

   (a) $f_1(\phi^* D_2)) = (\phi_* f_1)(D_2)$;

   (b) $f_2(\phi_* D_1)) = (\phi^* f_2)(D_1)$.

Skica dokaza. Dokaz celotne trditve je v nekaterih točkah enostaven, v ostalih pa dolg in tehničen, zato bomo samo podali skico dokaza.

1. Sledi direktno iz točke 1. v trditvi 3.2.13.

2. Sledi iz definicij in dejstva, da za vsako točko $P \in C_1$ velja $\mathrm{ord}_P(\phi^* f) = e_\phi(P)\mathrm{ord}_{\phi P}(f)$.

3. Sledi iz definicije stopnje (3.7) in ϕ_* (3.9).

4. Dokaz je na voljo v [86].

5. Sledi direktno iz definicije ϕ^*, ϕ_* in točke 1. v trditvi 3.2.13.

6. Prvi del sledi direktno iz točke 3. v trditvi 3.2.13, drugi del je očiten.

7. Dokaz je na voljo v [137, poglavje II.3].

■

Opomba: Iz trditve 3.3.12 sledi, da ϕ^* in ϕ_* slikata delitelje stopnje 0 v delitelje stopnje 0 ter glavne delitelje v glavne delitelje. Drugače povedano,

$$\phi^* : \mathrm{Pic}^0(C_2) \to \mathrm{Pic}^0(C_1)$$

in

$$\phi_* : \mathrm{Pic}^0(C_1) \to \mathrm{Pic}^0(C_2).$$

Opomba: Naj bo $f \in \overline{K}(C)$ nekonstantna funkcija na gladki krivulji C in $\ell : C \to \mathbb{P}^1$ pripadajoča preslikava (3.3). Iz definicije ℓ sledi

$$\mathrm{div}(f) = l^*((0) - (\infty)).$$

Potem je

$$\deg \mathrm{div}(f) = \deg \ell^*((0) - (\infty)) = \deg f - \deg f = 0. \tag{3.11}$$

Pomemben rezultat v teoriji deliteljev je tudi Weilov izrek o recipročnosti.

Izrek 3.3.13. *Naj bosta f in g neničelni funkciji na krivulji C nad K. Če sta podpori* $\mathrm{div}(f)$ *in* $\mathrm{div}(g)$ *disjunktni, velja*

$$f(\mathrm{div}(g)) = g(\mathrm{div}(f)).$$

Dokaz. Rezultat bomo najprej dokazali za primer premice $C = \mathbb{P}^1$. Točke

$$[x,z] = \begin{cases} [x/z, 1] & ; \text{z} \neq 0 \\ [1,0] & ; \text{z} = 0 \end{cases}$$

iz $\mathbb{P}^1(\overline{K})$ lahko identificiramo z $\{a \in \overline{K}\} \cup \{\infty\}$. Funkcija f na C je ulomek $u(x,z)/v(x,z)$ dveh homogenih polinomov nad $\overline{K}$ enakih stopenj. Dejansko se lahko omejimo na afino množico $z = 1$, in na f gledamo kot $u(x)/v(x)$, kjer sta $u(x), v(x) \in \overline{K}[x]$. Če je $f = \prod_{i=1}^{m}(x - a_i)^{n_{a_i}}$, potem je $\mathrm{div}(f) = \sum_{i=1}^{m} n_{a_i}(a_i) - n_\infty(\infty)$, kjer je $n_\infty = \sum_{i=1}^{m} n_{a_i} = \deg(u(x)) - \deg(v(x))$.

Naj bo f kot zgoraj in naj bo $g = \prod_{j=1}^{m'}(x - b_j)^{n_{b_j}}$. Privzemimo, da imata $\mathrm{div}(f)$ in $\mathrm{div}(g)$ disjunktni podpori brez točk v neskončnosti, kar pomeni, $a_i \neq b_j$ za vsak i, j in $\sum_{i=1}^{m} n_{a_i} = \sum_{j=1}^{m'} n_{b_j} = 0$. Potem velja

$$\begin{aligned} f(\mathrm{div}(g)) &= \prod_{j=1}^{m'}\prod_{i=1}^{m}(b_j - a_i)^{n_{a_i} n_{b_j}} \\ &= (-1)^{(\sum_{i=1}^{m}\sum_{j=1}^{m'} n_{a_i} n_{b_j})} \prod_{j=1}^{m'}\prod_{i=1}^{m}(a_i - b_j)^{n_{a_i} n_{b_j}} \\ &= g(\mathrm{div}(f)), \end{aligned}$$

kjer je predznak enak 1 zaradi $\sum_{i=1}^{m} n_{a_i} = \sum_{j=1}^{m'} n_{b_j} = 0$.

Če pa se ∞ pojavi v podpori enega izmed deliteljev $\mathrm{div}(f)$, $\mathrm{div}(g)$, potem sta stopnji $u(x)$ in $v(x)$ različni. V tem primeru definiramo $(\infty - b_i)/(\infty - b_j) = 1$ oziroma $(\infty - a_i)/(\infty - a_j) = 1$ in nadaljujemo kot zgoraj.

Za $C \neq \mathbb{P}^1$ pa dokažemo izrek takole. Naj bo $i = x/z$ funkcija identitete na $\mathbb{P}^1$. Potem je $\mathrm{div}(i) = (0) - (\infty)$ in po trditvi 3.3.12 dobimo $\mathrm{div}(g) = g^*(\mathrm{div}(i))$. Posledično velja

$$f(\mathrm{div}(g)) = f(g^*(\mathrm{div}(i))) = (g_* f)(\mathrm{div}(i)).$$

Ker je $g_* f$ funkcija na $\mathbb{P}^1$ po zgoraj dokazanem velja

$$(g_* f)(\mathrm{div}(i)) = i(\mathrm{div}(g_* f)).$$

Za dokončanje dokaza potrebujemo še naslednji izračun

$$i(\mathrm{div}(g_* f)) = (g^* i)(\mathrm{div}(f)) = i \circ g(\mathrm{div}(f)) = g(\mathrm{div}(f)).$$

■

Celotno teorijo deliteljev na ravninskih krivuljah je možno razviti s pomočjo Bezoutovega izreka. Med drugim Bezoutov izrek omogoča elegantno računanje deliteljev racionalnih funkcij.

Izrek 3.3.14. *(Bezout) [45]. Naj bosta C_1 in C_2 krivulji v $\mathbb{P}^2(\overline{K})$ podani kot ničli homogenih polinomov stopenj d_1 in d_2. Potem je*

$$\#(C_1 \cap C_2) = d_1 \cdot d_2.$$

■

Zgornji izrek nam v jeziku deliteljev pove, da je

$$\sum_{P \in C_1 \cap C_2} n_P = d_1 \cdot d_2.$$

S pomočjo Bezoutovega izreka lahko enostavno dokažemo enakost (3.11) za ravninske krivulje. Če je $f/g \in \overline{K}(C)$ racionalna funkcija, potem velja

$$\operatorname{div}\left(\frac{f}{g}\right) = \operatorname{div}(f) - \operatorname{div}(g) = (\{f = 0\} \cap C) - (\{g = 0\} \cap C)$$

in sledi

$$\deg \operatorname{div}\left(\frac{f}{g}\right) = 0.$$

V nadaljevanju bomo navedli Riemann-Rochov izrek, ki je eden ključnih izrekov algebraične geometrije krivulj. Potrebovali ga bomo za konstrukcijo grupe točk na krivuljah. Najprej pa definiramo nekaj struktur, ki nastopajo v Riemann-Rochovem izreku.

Definicija 3.3.15. Naj bo C projektivna krivulja. **Prostor diferencialnih form** Ω_C je $\overline{K}(C)$-vektorski prostor, generiran s simboli oblike dx, za katere veljajo pravila odvajanja: $d(x+y) = dx + dy$, $d(xy) = xdy + ydx$, za $x, y \in \overline{K}(C)$ ter $da = 0$ za $a \in \overline{K}$. Vsako formo $\omega \in \Omega_C$ lahko predstavimo z deliteljem $\operatorname{div}(\omega) \in \operatorname{Div}(C)$. Izkaže se, da poljubni $\omega \in \Omega_C$ definira isti razred delitelja v $\operatorname{Pic}(C)$. **Kanonični delitelj** na C definiramo kot $\operatorname{div}(\omega) \in \operatorname{Pic}(C)$.

Študij diferencialnih form presega okvir tega dela, opis je na voljo v [137, poglavje II].

Definicija 3.3.16. Za $D \in \operatorname{Div}(C)$ je **linearni sistem funkcij**

$$\mathcal{L}(D) = \{f \in \overline{K}(C)^* : \ \operatorname{div}(f) \geq -D\} \cup \{0\}.$$

Opazimo, da $\mathcal{L}(D)$ sestavljajo funkcije, ki imajo pole kvečjemu v D. Množica $\mathcal{L}(D)$ je končni vektorski prostor nad $\overline{K}$ [137, poglavje III] in njegovo dimenzijo označimo z $\ell(D) = \dim_{\overline{K}} \mathcal{L}(D)$. Pri računanju dimenzij linearnih sistemov nam koristi naslednja lema.

Lema 3.3.17. *Naj za izbrani $D \in \operatorname{Div}(C)$ velja $\deg D < 0$. Potem je $\mathcal{L}(D) = \{0\}$ in $\ell(D) = 0$.*

Dokaz. Izberimo neničelni $f \in \mathcal{L}(D)$. Ker je $\deg \operatorname{div}(f) = 0$ in $\operatorname{div}(f) \geq -D$, sledi

$$0 = \deg \operatorname{div}(f) \geq \deg(-D) = -\deg D$$

Posledično je $\deg D \geq 0$. Ker smo za izbrani D privzeli $\deg(D) < 0$, sledi $\mathcal{L}(D) = \{0\}$ in $\ell(D) = 0$. ■

Zdaj imamo definirano vse potrebno za Riemann-Rochov izrek. Dokaza zaradi dolžine in zahtevnosti ne bomo navajali, na voljo je v [60] ali [87].

Izrek 3.3.18. *(Riemann - Roch). Naj bo C gladka krivulja in K_C kanonični delitelj na C. Potem obstaja tako celo število $g \geq 0$, imenovano* **rod krivulje** *C, da je za vsak delitelj $D \in \operatorname{Div}(C)$ izpolnjena enakost*

$$\ell(D) - \ell(K_C - D) = \deg D - g + 1.$$

■

Posledica 3.3.19. *Veljajo naslednje trditve:*

1. $\ell(K_C) = g$;
2. $\deg K_C = 2g - 2$;
3. *Če je* $\deg D > 2g - 2$, *potem je* $\ell(D) = \deg D - g + 1$.

Dokaz.

1. Izberimo $D = 0$ in uporabimo Riemann-Rochov izrek 3.3.18, kjer upoštevamo, da je $\mathcal{L}(0) = \overline{K}$ in $\ell(0) = 1$.
2. Izberimo $D = K_C$ in uporabimo točko 1. zgoraj.
3. Prevzemimo, da je $\deg D > 2g - 2$. Potem iz točke 2. zgoraj sledi $\deg(K_C - D) < 0$ in po lemi 3.3.17 je $\ell(K_C - D) = 0$. Zdaj lahko uporabimo izrek 3.3.18.

■

Poglavje 4

ELIPTIČNE KRIVULJE

V tem poglavju si bomo ogledali eliptične krivulje. Spomnimo se, da so krivulje algebraične raznoterosti dimenzije 1, zato zanje veljajo vse lastnosti, ki veljajo za splošne algebraične raznoterosti. Eliptične krivulje so algebraične krivulje rodu 1 (rod smo definirali v Riemann-Rochovem izreku 3.3.18).

Najprej bomo obravnavali ravninske eliptične krivulje, definirane v $\mathbb{P}^2$ kot množica rešitev Weierstrassove enačbe. Nato bomo uvedli strukturo grupe na eliptični krivulji. Pri tem bomo dokazali, da sta tako definirana grupa in Picardova grupa deliteljev izomorfni, kar je bistveno za razumevanje računanja parjenj v 5. poglavju. Nadaljevali bomo z opisom izogenij, ovojev in torzijskih točk. Posebej bomo predstavili eliptične krivulje nad končnimi obsegi, ki se uporabljajo v kriptografiji. Podrobneje si bomo ogledali tudi razdelitev na supersingularne in navadne krivulje. Poglavje bomo zaključili z definicijo kompleksnega množenja, ki služi za konstrukcije krivulj.

V tem in naslednjih poglavjih bomo zaradi lažjega zapisa $\mathbb{Z}/n\mathbb{Z}$ pogosto označevali z $\mathbb{Z}_n$.

4.1 Weierstrassove enačbe

V $\mathbb{P}^2$ si oglejmo množico rešitev naslednje kubične enačbe:

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3, \tag{4.1}$$

kjer so $a_1, \ldots, a_6 \in \overline{K}$. Enačbam take oblike pravimo **Weierstrassove** enačbe. Opazimo, da je $[0, 1, 0]$ edina točka krivulje, ki leži v ∞ glede na afino ravnino $z \neq 0$. Za lažjo notacijo, bomo uporabili nehomogene koordinate $x = X/Z$ in $y = Y/Z$. Zgornja enačba (4.1) se prevede v

$$E: \ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{4.2}$$

Taki enačbi pravimo tudi **splošna Weierstrassova enačba.** Če je $\mathrm{char}(\overline{K}) \neq 2$, lahko splošno Weierstrassovo enačbo (4.2) poenostavimo s preprosto substitucijo $y \mapsto 1/2(y - a_1x - a_3)$ in dobimo

$$E: \ y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6, \tag{4.3}$$

kjer so

$$\begin{aligned} b_2 &= a_1^2 + 4a_2, \\ b_4 &= 2a_4 + a_1a_3, \\ b_6 &= a_3^2 + 4a_6. \end{aligned} \tag{4.4}$$

Vpeljimo še naslednje oznake, ki jih bomo uporabljali v nadaljevanju:

$$\begin{aligned} b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2, \\ c_4 &= b_2^2 - 24b_4, \\ c_6 &= -b_2^3 + 36b_2b_4 - 216b_6, \\ \Delta &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6, \\ j &= \tfrac{c_4^3}{\Delta}, \\ \omega &= \tfrac{dx}{2y+a_1x+a3} = \tfrac{dy}{3x^2+2a_2x+a_4-a_1y}. \end{aligned} \tag{4.5}$$

Iz zgornjih definicij sledita zvezi:

$$\begin{aligned} 4b_8 &= b_2b_6 - b_4^2 \\ 1728\Delta &= c_4^3 - c_6^2. \end{aligned}$$

Če je $\mathrm{char}(\overline{K}) \neq 2, 3$, potem lahko enačbo (4.3) z zamenjavo $x \mapsto (x - 3b_2)/36$ in $y \mapsto y/108$ prevedemo na

$$E: \; y^2 = x^3 - 27c_4x - 54c_6. \tag{4.6}$$

Definicija 4.1.1. Vrednosti $\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6$ pravimo **diskriminanta** Weierstrassove enačbe, vrednosti $j = \dfrac{c_4^3}{\Delta}$ pravimo **j-invarianta** eliptične krivulje E in $\omega = \dfrac{dx}{2y + a_1x + a3} = \dfrac{dy}{3x^2 + 2a_2x + a_4 - a_1y}$ je **invariantni diferencial** povezan z Weierstrassovo enačbo.

Kdaj je Weierstrassova enačba eliptične krivulje enolična, nam pove naslednji izrek.

Izrek 4.1.2. *[137, trditev III.3.1] Na eliptični krivulji E nad obsegom K izberimo točko $\mathcal{O} \in E(K)$.*

1. *Obstajata taki funkciji $X, Y \in K(E)$, da preslikava*

$$\phi : E \to \mathbb{P}^2, \quad \phi = [X, Y, 1]$$

porodi izomorfizem med krivuljo E/K in krivuljo z Weierestrassovo enačbo

$$E_W: \; y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Poleg tega velja $\phi(\mathcal{O}) = [0, 1, 0]$, ki je edina točka v ∞ na E_W. Taki funkciji X in Y imenujemo **Weierestrassovi koordinatni funkciji** *na krivulji E.*

2. *Poljubni Weierstrassovi enačbi E_W in $E_{W'}$ za krivuljo E sta povezani z linearno transformacijo spremenljivk*

$$x = u^2x' + r, \quad y = u^3y' + su^2x' + t,$$

kjer so $u, r, s, t \in K$ in $u \neq 0$.

■

Če za linearno transformacijo v točki 2. trditve 4.1.2 izračunamo vse nove koeficiente a_i' in vrednosti Δ', j', ω', vidimo, da je $j' = j$. Od tod j-invarianta dobi tudi ime, saj je invarianta izomorfnega razreda krivulje.

Zaradi lažjega zapisa se v primerih, ko je $\text{char}(K) \neq 2, 3$, uporablja tudi naslednja oblika Weierestrassove enačbe

$$E: \ y^2 = x^3 + Ax + B.$$

Pripadajoči vrednosti Δ in j sta potem enaki

$$\Delta = -16(4A^3 + 27B^2), \quad j = \frac{-1728(4A)^3}{\Delta}. \tag{4.7}$$

Izrek 4.1.3.

1. *Za krivuljo z Weierestrassovo enačbo* (4.2) *velja:*
   (a) *Krivulja je nesingularna natanko tedaj, ko je $\Delta \neq 0$;*
   (b) *Pri vrednostih $\Delta = 0$ in $c_4 \neq 0$, ali $\Delta = c_4 = 0$, obstaja natanko ena singularna točka.*
2. *Dve gladki eliptični krivulji nad obsegom $\overline{K}$ sta izomorfni natanko tedaj, ko imata enaki j-invarianti.*
3. *Za vsak $j_0 \in \overline{K}$ obstaja gladka eliptična krivulja definirana nad obsegom $K(j_0)$ z j-invarianto enako j_0.*

Dokaz.

1. Naj bo E krivulja z Weierstrassovo enačbo

$$E: \ f(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0.$$

Najprej bomo pokazali, da točka v neskončnosti nikoli ni singularna. V homogeni enačbi

$$F(X, Y, Z) = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z + a_4XZ^2 - a_6Z^3 = 0$$

ima točka v ∞ koordinate $\mathcal{O} = [0, 1, 0]$. Iz $\partial F/\partial Z(\mathcal{O}) = 1 \neq 0$ sklepamo, da $\mathcal{O}$ ni singularna točka krivulje. Naj bo zdaj E singularna v točki $P_0 = (x_0, y_0)$. Substitucija $x \mapsto x' + x_0$, $y \mapsto y' + y_0$ ohrani vrednosti invariant j, Δ in c_4, zato

lahko brez škode za splošnost predpostavimo, da je $P_0 = (0,0)$. Potem velja $a_6 = f(0,0) = 0$, $a_4 = \partial f/\partial x(0,0) = 0$, $a_3 = \partial f/\partial y(0,0) = 0$ in enačba za E ima obliko

$$E: \ f(x,y) = y^2 + a_1xy - a_2x^2 - x^3 = 0.$$

Od tod razberemo

$$c_4 = (a_1^2 + 4a_2)^2 \ \text{ in } \ \Delta = 0.$$

Kvadratna forma $y^2 + a_1xy - a_2x^2$ je produkt dveh enakih ali različnih linearnih faktorjev pri pogoju $a_1^2 + 4a_2 = 0$ oziroma $a_1^2 + 4a_2 \neq 0$. V teh primerih je E singularna v točki $(0,0)$.

Dokažimo zdaj še obrat. Preveriti moramo, da je $\Delta \neq 0$ za gladko E. Zaradi enostavnosti predpostavimo, da je $\mathrm{char}(K) \neq 2$. Tako Weierestrassova enačba dobi obliko

$$E: \ y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6.$$

Podobno kot zgoraj preverimo, da je E singularna natanko tedaj, ko obstaja točka $(x_0, y_0) \in E$, ki zadošča

$$2y_0 = 12x_0^2 + 2b_2x_0 + 2b_4 = 0.$$

Singularne točke so torej ravno točke oblike $(x_0, 0)$, kjer je x_0 dvojni koren $4x^3 + b_2x^2 + 2b_4x + b_6 = 0$. Ta kubični polinom pa ima dvojno ničlo natanko takrat, ko je njegova diskriminanta, ki je 16Δ, enaka 0. Ker kubični polinom ne more imeti dveh dvojnih ničel, ima E lahko kvečjemu eno singularno točko.

2. Če sta dve gladki eliptični krivulji izomorfni, potem transformacija v izreku 4.1.2 ohranja vrednosti j-invariante. Za dokaz bomo predpostavili, da je $\mathrm{char}(K) \neq 2, 3$. Naj bosta E in E' eliptični krivulji Weierestrassove oblike z enako j-invarianto in enačbama

$$E: \ y^2 = x^3 + Ax + B,$$
$$E': \ (y')^2 = (x')^3 + A'x' + B'.$$

Za $j = j'$ sledi,

$$A^3B'^2 = A'^3B^2.$$

Izomorfizem med E in E' je torej oblike $(x,y) = (u^2x', u^3y')$. Ločimo tri primere:

   (a) $A = 0$ natanko tedaj, ko je $j = 0$. Ker je $\Delta \neq 0$ mora biti $B \neq 0$, zato je tudi $A' = 0$. Izomorfizem dobimo, če za u vzamemo vrednost $u = (B/B')^{1/6}$.

   (b) $B = 0$ natanko tedaj, ko je $j = 1728$. Potem je $A' \neq 0$ in $B' = 0$, torej za u vzamemo $u = (A/A')^{1/4}$.

   (c) $AB \neq 0$ natanko tedaj, ko je $j \neq 0$ in 1728. Potem je tudi $A'B' \neq 0$. Za u vzamemo $u = (A/A')^{1/4} = (B/B')^{1/6}$.

3. Naj bo $j_0 \neq 0$ in 1728. Za naslednjo krivuljo

$$E: \ y^2 + xy = x^3 - \frac{36}{j_0 - 1728}x - \frac{1}{j_0 - 1728}$$

izračunajmo pripadajoče invariante

$$\Delta = \frac{j_0^2}{(j_0 - 1728)^3} \quad \text{in} \quad j = j_0.$$

V primeru $j_0 = 0$ vzamemo krivuljo

$$E: \ y^2 + y = x^3 \ \text{ z invariantama } \ \Delta = -27, j = 0.$$

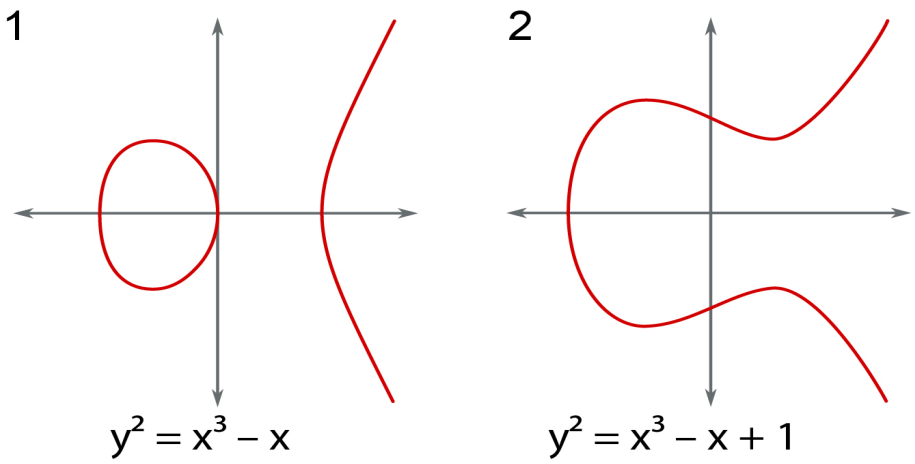
V primeru $j_0 = 1728$ pa vzamemo krivuljo

$$E: \ y^2 = x^3 + x \ \text{ z invariantama } \ \Delta = -64, j = 1728.$$

V obsegu s karakteristiko 2 ali 3, je 1728 enako 0. Pri $\text{char}(K) = 2$ je gladka prva, pri $\text{char}(K) = 3$ pa druga izmed zgornjih dveh krivulj.

■

Na sliki 4.1 sta dva primera eliptičnih krivulj.

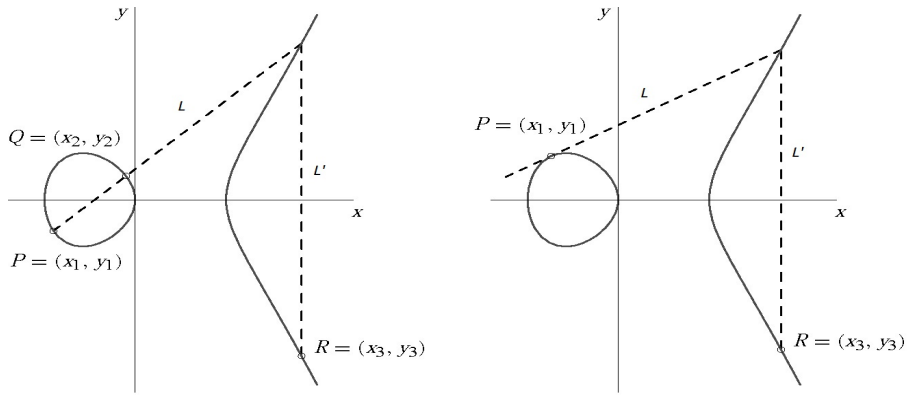


Slika 4.1: Primera eliptičnih krivulj.

4.2 Grupa na eliptični krivulji

Naj bo E eliptična krivulja podana z Weierstrassovo enačbo. Spomnimo se, da je krivulja $E \subset \mathbb{P}^2$ sestavljena iz afinih točk $P = (x, y)$, ki zadoščajo enačbi pri $z = 1$ skupaj s točko v neskončnosti $\mathcal{O} = [0, 1, 0]$. Naj bo $L \subset \mathbb{P}^2$ premica. Ker ima polinom za E stopnjo 3, premica L po Bezoutovem izreku 3.3.14 seka E natanko v 3 točkah. Presečne točke niso nujno različne, kar se zgodi, ko je L tangenta na E. Definirajmo operacijo $\oplus$ na E z naslednjim pravilom:

Definicija 4.2.1. Izberimo točki $P, Q \in E$. Naj bo L premica skozi P in Q (tangenta, če je $P = Q$) in R' tretja točka, kjer L seka E. Naj bo L' premica skozi R' in točko v neskončnosti $\mathcal{O}$. Naj bo R tretje presečišče L' s krivuljo E. Potem definiramo $P \oplus Q = R$.



(a) $P \oplus Q = R$. (b) $P \oplus P = R$.

Slika 4.2: Seštevanje točk na elitpični krivulji.

Definicija operacije $\oplus$ je nazorno vidna tudi na sliki 4.2. Trditev 4.2.2 pa nam opiše lastnosti operacije $\oplus$ na točkah krivulje E.

Trditev 4.2.2. *Operacija $\oplus$ ima naslednje lastnosti:*

1. *Če premica L seka krivuljo E v ne nujno različnih točkah P, Q, R', potem velja*

$$(P \oplus Q) \oplus R' = \mathcal{O};$$

2. *$P \oplus \mathcal{O} = P$ za vsak $P \in E$;*
3. *$P \oplus Q = Q \oplus P$ za vsak $P, Q \in E$;*
4. *Naj bo $P \in E$. Potem obstaja taka točka $P \in E'$, da velja $P \oplus P' = \mathcal{O}$;*
5. *Za točke $P, Q, R \in E$ velja $(P \oplus Q) \oplus R = P \oplus (Q \oplus R)$.*

Dokaz. Vse trditve preverimo s pomočjo slike 4.2.

1. Sledi iz definicije 4.2.1.
2. Če v definiciji 4.2.1 vzamemo $Q = \mathcal{O}$, vidimo da se premici L in L' ujemata. Prva seka krivuljo E v točkah $P, \mathcal{O}, R'$, druga pa v točkah $R', \mathcal{O}, P \oplus \mathcal{O}$, torej je $P \oplus \mathcal{O} = P$.
3. Sledi iz simetričnost konstrukcije v definiciji $\oplus$.
4. Naj premica skozi P in $\mathcal{O}$ seka krivuljo v točki R'. Z uporabo točk 1. in 2. dobimo $\mathcal{O} = (P \oplus \mathcal{O}) \oplus R' = P \oplus R'$.

5. Dokaz asociativnosti je bolj zahteven in je zajet v izreku 4.2.7, ki je posledica Riemann-Rochovega izreka. Asociativnost je možno izpeljati tudi iz eksplicitnih formul za seštevanje na eliptični krivulji.

■

Trditev 4.2.2 nam pove, da točke na krivulji E skupaj z operacijo $\oplus$ tvorijo Abelovo grupo z nevtralnim elementom $\mathcal{O}$. Naslednja trditev to eksplicitno potrdi za krivulje definirane z Weierstrassovo enačbo nad obsegom K.

Trditev 4.2.3. *Naj bo E definirana nad obsegom K. Potem je*

$$E(K) = \{(x, y) \in K^2 : \ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{\mathcal{O}\}$$

podgrupa v $E = E(\overline{K})$ glede na operacijo $\oplus$.

Dokaz. Če imata P in Q koordinate v obsegu K, potem ima koeficiente v K tudi enačba premice, ki ju povezuje. Če je E definirana nad K potem bo tretja presečna točka imela koordinate, ki bodo racionalne funkcije koeficientov premice in krivulje E, torej bodo tudi v obsegu K. Eksplicitni dokaz bomo podali v nadaljevanju, ko bomo pravilo seštevanja tudi eksplicitno zapisali. ■

V nadaljevanju bomo namesto $\oplus$ pisali $+$, poleg tega bomo uporabljali še oznake $mP = \underbrace{P + \ldots + P}_{m \in \mathbb{N}}$, $0P = \mathcal{O}$ in $-P + P = \mathcal{O}$.

Kot že omenjeno bomo v nadaljevanju uporabljali eksplicitne formule za seštevanje točk na eliptični krivulji. Formule bomo zapisali v obliki trditve, dokaz pa je na voljo v [137].

Trditev 4.2.4. *[137, Pravilo III.2.3]. Naj bo E eliptična krivulja v Weierstrassovi obliki*

$$E : \ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

1. *Za izbrano $P_0 = (x_0, y_0) \in E$ je $-P_0 = (x_0, -y_0 - a_1x_0 - a_3)$.*

V nadaljevanju označimo $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$, $P_3 = (x_3, y_3)$ in naj bo $P_1 + P_2 = P_3$.

2. *V primeru $x_1 = x_2$ in $y_1 + y_2 + a_1x_2 + a_3 = 0$ velja $P_1 + P_2 = \mathcal{O}$. Sicer definirajmo:*

$$(\lambda, \nu) = \begin{cases} \left(\dfrac{y_2 - y_1}{x_2 - x_1}, \dfrac{y_1x_2 - y_2x_1}{x_2 - x_1}\right), & \text{če } x_1 \neq x_2; \\ \left(\dfrac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}, \dfrac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3}\right), & \text{če } x_1 = x_2. \end{cases}$$

Potem je $y = \lambda x + \nu$ premica skozi P_1 in P_2 oziroma tangenta na E v $P_1 = P_2$.

3. *Točka $P_3 = P_1 + P_2$ ima koordinati*

$$\begin{aligned} x_3 &= \lambda^2 + a_1\lambda - a_2 - x_1 - x_2, \\ y_3 &= -(\lambda + a_1)x_3 - \nu - a_3. \end{aligned}$$

4. *Če* $P_1 \neq \pm P_2$, x_3 *izračunamo po formuli:*

$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 + a_1\left(\frac{y_2 - y_1}{x_2 - x_1}\right) - a_1 - x_1 - x_2.$$

Če je $P_1 = P_2$ *pa* x_3 *dobimo iz formule:*

$$x_3 = \frac{x^4 - b_4x^2 - 2b_6x - b_8}{4x^3 + b_2x^2 + 2b_4x + b_6},$$

kjer so b_2, b_4, b_6 *in* b_8 *definirani v* (4.4) *in* (4.5).

■

Grupo na eliptični krivulji lahko uvedemo tudi s pomočjo Riemann-Rochovega izreka. Ta grupa se ujema z zgoraj opisano grupo na Weierstrassovi kubiki.

Trditev 4.2.5. *Vsaka gladka krivulja* C *podana z Weierstrassovo enačbo* (4.1)*, je eliptična krivulja.*

Dokaz. Naj bo E množica rešitev Weierstrassove enačbe. Invariantni diferencial je po definiciji 4.1.1 enak

$$\omega = \frac{dx}{2y + a_1x + a_3} \in \Omega_{\cdot}C$$

Ker ω nima ničel in polov, je $\operatorname{div}(\omega) = 0$. Po Riemmann-Rochovem izreku 3.3.18 pa je

$$2 \cdot \operatorname{rod}(E) - 2 = \deg \operatorname{div}(\omega).$$

Posledično je $\operatorname{rod}(E) = 1$, kar je definicija eliptične krivulje. ■

Zdaj bomo uporabili Riemmann-Roch izrek še za vpeljavo pravil seštevanja na točkah krivulje E.

Lema 4.2.6. *Naj bo* C *krivulja rodu 1 in naj bosta* $P, Q \in C$*. Potem sta* $(Q) \sim (P)$ *ekvivalentna delitelja natanko tedaj, ko je* $P = Q$*.*

Dokaz. Naj bosta $(P) \sim (Q)$ in izberimo $f \in \overline{K}(C)$, tako da je $\operatorname{div}(f) = (P) - (Q)$. Iz definicije 3.3.16 linearnega sistema sledi da je $f \in \mathcal{L}((Q))$. Po Riemmann-Rochovem izreku velja $\dim_{\overline{K}}\mathcal{L}((Q)) = 1$. Ker pa $\mathcal{L}((Q))$ že vsebuje konstantno funkcijo, sledi da je f konstantna funkcija in $P = Q$. ■

Izrek 4.2.7. *Naj bo* E *eliptična krivulja skupaj z izbrano točko* $\mathcal{O}$*.*

1. *Za vsak delitelj* $D \in \operatorname{Div}^0(E)$ *obstaja enolično določena točka* $P \in E$*, tako da je* $D \sim (P) - (\mathcal{O})$*.*

2. *Preslikava* $\sigma : \operatorname{Div}^0(E) \to E$ *definirana s predpisom* $\sigma(D) = P$ *za* $D \sim (P) - (\mathcal{O})$ *je surjektivna.*

3. *Naj bosta* $D_1, D_2 \in \operatorname{Div}^0(E)$*, Potem je* $\sigma(D_1) = \sigma(D_2)$ *natanko tedaj, ko je* $D_1 \sim D_2$*. Torej je inducirana kvocientna preslikava* $\sigma : \operatorname{Pic}^0(E) \to E$ *bijekcija.*

4. *Inverz od σ iz točke 3. je preslikava*

$$\begin{array}{rccc} \kappa: & E & \to & \mathrm{Pic}^0(E), \\ & P & \mapsto & (P)-(\mathcal{O}). \end{array}$$

5. *Če je E podana z Weierstrassovo enačbo, potem se operacija seštevanje v definiciji 4.2.1 ujema s seštevanjem porojenim iz* $\mathrm{Pic}^0(E)$ *z uporabo σ.*

Dokaz.

1. Ker ima E rod 1, je po posledici 3.3.19 Riemmann-Rochovega izreka $\dim_{\overline{K}}\mathcal{L}(D+(\mathcal{O}))=1$. Naj bo $f\in\overline{K}(E)$ generator za $\mathcal{L}(D+(\mathcal{O}))$. Po definiciji 3.3.16 linearnega sistema $\mathcal{L}$ je $\mathrm{div}(f)\geq -D-(\mathcal{O})$ in po (3.11) velja $\deg(\mathrm{div}(f))=0$, sledi $\mathrm{div}(f)=-D-(\mathcal{O})+(P)$ za nek $P\in E$. Torej je $D\sim(P)-(\mathcal{O})$, kar nam da eksistenco točke P z želenimi lastnostmi. Dokazati moramo še enoličnost. Naj bo $P'\in E$ točka z enakimi lastnostmi. Potem $(P)\sim(D)+(\mathcal{O})\sim(P')$ in iz leme 4.2.6 sledi $P=P'$.

2. Za vsako točko $P\in E$ velja, $\sigma((P)-(\mathcal{O}))=P$.

3. Naj bosta $D_1,D_2\in\mathrm{Div}^0(E)$ in $P_i=\sigma(D_i)$. Iz definicije σ sledi $(P_1)-(P_2)\sim D_1-D_2$. Če je $P_1=P_2$, potem je očitno $D_1\sim D_2$. Obratno, $D_1\sim D_2$ implicira $(P_1)\sim(P_2)$ in po lemi 4.2.6 je $P_1=P_2$.

4. Sledi iz definicije $\sigma:\mathrm{Pic}^0(E)\to E$.

5. Naj bo E množica rešitev Weierstrassove enačbe in naj bosta $P,Q\in E$. Za dokaz bo zadoščalo, da preverimo

$$\kappa(P+Q)=\kappa(P)+\kappa(Q),$$

kjer je prva operacija + seštevanja na E iz definicije 4.2.1, druga operacija + pa je seštevanje razredov deliteljev v $\mathrm{Pic}^0(E)$. Naj bo $f(X,Y,Z)=\alpha X+\beta Y+\gamma Z=0$ enačba premice L v $\mathbb{P}^2$ skozi točki P in Q. Označimo z R tretjo točko kjer L seka krivuljo E. Naj bo $f'(X,Y,Z)=\alpha' X+\beta' Y+\gamma' Z=0$ enačba premica L' skozi $\mathcal{O}$ in R. Opazimo še, da premica $Z=0$ seka E v točki $\mathcal{O}$ z večkratnostjo 3. Potem iz definicije seštevanja 3.2.6 sledi $\mathrm{div}(f/Z)=(P)+(Q)+(R)-3(\mathcal{O})$ in $\mathrm{div}(f'/Z)=(R)+(\mathcal{O})+(P+Q)-3(\mathcal{O})$. Posledično velja $(P+Q)-(P)-(Q)+(\mathcal{O})=\mathrm{div}(f'/f)\sim 0$. Torej je $\kappa(P+Q)-\kappa(P)-\kappa(Q)=0$.

■

Posledica 4.2.8. *Naj bo E eliptična krivulja in naj bo $D=\sum n_P(P)\in\mathrm{Div}(E)$. D je glavni delitelj natanko tedaj, ko je $\sum n_P=0$ in $\sum n_P P=\mathcal{O}$.*

Dokaz. Zaradi enakosti (3.11) ima vsak glavni delitelj stopnjo enako 0. Izberimo $D=\sum_P n_P(P)\in\mathrm{Div}^0(E)$. Iz izreka 4.2.7 sledi

$$D\sim 0\Leftrightarrow\sigma(D)=0\Leftarrow\sum n_P\cdot\sigma((P)-(\mathcal{O})=0,$$

kar je natanko to, kar želimo dokazati, saj je $\sigma((P)-(\mathcal{O}))=P$. ■

Primer. Naj bo $E:\ y^2 = x^3 + 4x$ eliptična krivulja and obsegom $\mathbb{F}_{11}$. Izberimo delitelj

$$D = ((0,0)) + ((2,4)) + ((4,5)) + ((6,3)) - 4(\mathcal{O})$$

Stopnja $\deg D = 0$ in $(0,0) + (2,4) + (4,5) + (6,3) - 4\mathcal{O} = \mathcal{O}$. Po posledici 4.2.8 je $D = \operatorname{div}(f)$ glavni delitelj. Zdaj bomo racionalno funkcijo $f \in \overline{K}(E)$ tudi skonstruirali. Premica skozi točki $(0,0)$ in $(2,4)$ ima enačbo $y - 2x = 0$. Ta premica je tangenta na E v točki $(2,4)$, zato da je njen delitelj enak

$$\operatorname{div}(y - 2x) = ((0,0)) + 2((2,4)) - 3(\mathcal{O}).$$

Navpična premica skozi $(2,4)$ je $x - 2 = 0$ in njen delitelj je enak

$$\operatorname{div}(x - 2) = ((2,4)) + ((2,-4)) - 2(\mathcal{O}).$$

Če sestavimo vse tri delitelje, dobimo naslednje:

$$D = ((2,-4)) + \operatorname{div}\left(\frac{y-2x}{x-2}\right) + ((4,5)) + ((6,3)) - 3(\mathcal{O}).$$

Podobno dokažemo

$$((4,5)) + ((6,3)) = ((2,4)) + (\mathcal{O}) + \operatorname{div}\left(\frac{y+x+2}{x-2}\right).$$

Od tod sledi

$$D = ((2,-4)) + \operatorname{div}\left(\frac{y-2x}{x-2}\right) + ((2,4)) + \operatorname{div}\left(\frac{y+x+2}{x-2}\right) - 2(\mathcal{O}),$$

oziroma

$$\begin{aligned} D &= \operatorname{div}(x-2) + \operatorname{div}\left(\tfrac{y-2x}{x-2}\right) + ((2,4)) + \operatorname{div}\left(\tfrac{y+x+2}{x-2}\right) \\ &= \operatorname{div}\left(\tfrac{(y-2x)(y+x+2)}{x-2}\right). \end{aligned}$$

Iz računa

$$\begin{aligned} \tfrac{y^2+xy+2y-2xy-2x^2-4x}{x-2} &= \tfrac{y^2+2y-xy-2x^2-4x}{x-2} \\ &= \tfrac{y^2-2x^2-4x}{x-2} - y \\ &= \tfrac{4x+x^3-2x^2-4x}{x-2} - y \\ &= x^2 - y \end{aligned} \tag{4.8}$$

sklepamo, da se funkciji $\frac{(y-2x)(y+x+2)}{x-2}$ in $x^2 - y$ ujemata na krivulji $E:\ y^2 = x^3 + 4x$. Končni rezultat je torej

$$D = \operatorname{div}(x^2 - y).$$

•

Če združimo izrek 4.2.7 in zaporedje (3.8) na strani 26, dobimo

$$1 \to \overline{K}^* \to \overline{K}(E)^* \xrightarrow{\operatorname{div}} \operatorname{Div}^0(E) \xrightarrow{\sigma} E \to 0. \tag{4.9}$$

Zdaj bomo dokazali, da je seštevanje na krivulji smiselno definirano.

Izrek 4.2.9. *Naj bo E/K eliptična krivulja. Eksplicitna pravila za seštevanje opisana v trditvi 4.2.4 tvorijo naslednja morfizma:*

$$\begin{array}{rccc} +: & E\times E & \to & E \\ & (P_1,P_2) & \mapsto & P_1+P_2 \end{array} \quad in \quad \begin{array}{rccc} -: & E & \to & E \\ & P & \mapsto & -P. \end{array}$$

Dokaz. Najprej si oglejmo odštevanje. Preslikava

$$(x,y)\mapsto (x,-y-a_1x-a_3)$$

je racionalna preslikava $E\to E$ in ker je E gladka krivulja, je to morfizem po trditvi 3.2.6. Fiksirajmo zdaj točko $Q\neq\mathcal{O}$ na krivulji E in si oglejmo **translacijo** za Q

$$\begin{array}{rccc} \tau: & E & \to & E, \\ & P & \mapsto & P+Q. \end{array}$$

Po eksplicitnih formulah za seštevanje v trditvi 4.2.4 je to racionalna preslikava in po trditvi 3.2.6 je to morfizem. Ker ima inverz, ki je enak $P\mapsto P-Q$, je τ izomorfizem. Poglejmo si zdaj preslikavo seštevanja $+: E\times E\to E$. Iz formul za seštevanje v trditvi 4.2.4 vidimo, da je $+$ morfizem, razen morda v točkah: $(P,-P)$, $(P,\mathcal{O})$, (P,P) in $(\mathcal{O},P)$. V preostalih točkah sta namreč racionalni funkciji

$$\lambda=(y_2-y_1)/(x_2-x_1),\quad \nu=(y_1x_2-y_2x_1)/(x_2-x_1)$$

na $E\times E$ dobro definirani.

Izjemne točke lahko zaobidemo z računom podobnim kot (4.8). Tak pristop je dolgotrajen in tehničen, zato bomo raje izbrali pristop iz [137].

Naj bosta τ_1 in τ_2 translaciji za Q_1 in Q_2. Poglejmo si naslednji kompozitum preslikav:

$$\phi: E\times E\overset{\tau_1\times\tau_2}{\longrightarrow} E\times E\overset{+}{\longrightarrow} E\overset{\tau_1^{-1}}{\longrightarrow} E\overset{\tau_2^{-1}}{\longrightarrow} E.$$

Ker za seštevanje v Abelovi grupi veljata asociativnost in komutativnost (po trditvi 4.2.2), ϕ deluje po točkah na naslednji način:

$$(P_1,P_2)\overset{\tau_1\times\tau_2}{\longmapsto}(P_1+Q_1,P_2+Q_2)\overset{+}{\longmapsto}P_1+Q_1+P_2+Q_2\overset{\tau_1^{-1}}{\longmapsto}P_1+P_2+Q_2\overset{\tau_2^{-1}}{\longmapsto}P_1+P_2.$$

Racionalna preslikava ϕ se torej ujema s seštevanjem točk na E povsod, kjer je definirana.

Ker so τ_i izomorfizmi, je ϕ definiran povsod, razen v točkah $(P-Q_1,P-Q_2)$, $(P-Q_1,-P-Q_2)$, $(P-Q_1,-Q_2)$ in $(-Q_1,P-Q_2)$. Ker pa smo Q_1 in Q_2 izbrali poljubno, lahko z izbiro le teh najdemo končno množico preslikav

$$\phi_1,\phi_2,\ldots,\phi_n:\ E\times E\to E,$$

za katere velja:

1. ϕ_i je preslikava seštevanja iz trditve 4.2.4 povsod kjer je ϕ_i definirana;
2. Za vsak par točk $(P_1,P_2)\in E\times E$, obstaja i, za katerega je ϕ_i definiran v (P_1,P_2);

3. Če sta ϕ_i in ϕ_j oba definirana v (P_1, P_2), potem je $\phi_i(P_1, P_2) = \phi_j(P_1, P_2)$.

Tako smo seštevanje definirali na vseh parih točk na $E \times E$ in pokazali, da je morfizem. ■

Dejstvo, da točke eliptične krivulje tvorijo Abelovo grupo, je uporabljeno v večini protokolov na eliptičnih krivuljah. Zato je nujno, da o teh grupah povemo kaj več. Strnjeno veljajo naslednje lastnosti, od katerih bomo določene podrobneje predstavili v nadaljnjih razdelkih.

1. Eliptična krivulja nad končnim obsegom ima končno mnogo točk s koordinatami v tem obsegu. Pripadajoča grupa je končna Abelova grupa.

2. Če je E definirana nad obsegom $\mathbb{Q}$, potem je $E(\mathbb{Q})$ po Mordell-Weilovem izreku [137, 152] končno generirana Abelova grupa. Bolj natančno, $E(\mathbb{Q})$ je izomorfna grupi $\mathbb{Z}^r \oplus F$ za nek $r \geq 0$ in neko končno grupo F. Številu r pravimo **rang** $E(\mathbb{Q})$ in v splošnem je računanje vrednosti zelo zahtevno Ali je r lahko poljubno velik je še vedno odprt problem. Končno grupo F pa lahko enostavno generiramo s pomočjo Lutz-Nagellovega izreka [137, 152]. Še več, izrek Mazurja [98] pravi, da je takih grup lahko le končno mnogo.

3. Eliptična krivulja nad obsegom kompleksnih števil $\mathbb{C}$ je izomorfna torusu [152, poglavje 9].

4. Če je E definirana nad $\mathbb{R}$, je $E(\mathbb{R})$ izomorfna enotski krožnici S^1 ali $S^1 \times \mathbb{Z}_2$ [152, poglavje 9].

Od zdaj naprej bo eliptična krivulja za nas pomenila algebraično krivuljo rodu 1 opremljeno s strukturo grupe, v kateri nevtralni element označimo z $\mathcal{O}$ in mu rečemo točka v neskončnosti.

V poglavju 5 bomo delitelju priredili vsoto njegovih točk. Za delitelj $D = \sum_P n_P(P) \in \mathrm{Div}(E)$ definiramo **vsoto** kot

$$sum(D) = \sum_{P \in E} n_P P \in E. \tag{4.10}$$

4.3 Izogenije

Definicija 4.3.1. Naj bosta E_1 in E_2 eliptični krivulji z izbranima točkama v neskončnosti $\mathcal{O}_1$ in $\mathcal{O}_2$. **Izogenija** med E_1 in E_2 je morfizem $\phi : E_1 \to E_2$, za katerega velja $\phi(\mathcal{O}_1) = \mathcal{O}_2$. Krivulji E_1 in E_2 sta izogeni, če med njima obstaja taka izogenija ϕ, da je $\phi(E_1) \neq \{\mathcal{O}_2\}$.

Iz lastnosti morfizmov nad algebraičnimi raznoterostmi v trditvi 3.2.7 sledi, da za izogenijo velja $\phi(E_1) = \{\mathcal{O}_2\}$, ali $\phi(E_1) = E_2$. Tako ima vsaka neničelna izogenija končno stopnjo. Po izreku 3.2.8 ϕ porodi injekcijo obsegov funkcij $\phi^* : \overline{K}(E_2) \to \overline{K}(E_1)$.

Ker eliptične krivulje dopuščajo strukturo grupe, izogenije med njimi tvorijo grupo $\mathrm{Hom}(E_1, E_2)$. Da je $\mathrm{Hom}(E_1, E_2)$ s seštevanjem $(\phi+\psi)(P) = \phi(P)+\psi(P)$ res grupa, nam zagotavlja izrek 4.2.9. Če je $E_1 = E_2$ lahko prav tako tvorimo izogenije. V tem primeru

označimo $\mathrm{End}(E) = \mathrm{Hom}(E_1, E_2)$ **kolobar endomorfizmov** za množenje definirano kot $(\phi \circ \psi)(P) = \phi(\psi(P))$. Obrnljivi elementi tega kolobarja tvorijo grupo avtomorfizmov.

Za vsak $m \in \mathbb{Z}$ lahko definiramo **izogenijo množenja** z m kot $[m] : E \to E,\ [m]P = \underbrace{P + P + \ldots + P}_{m}$. Opazimo, da je $[0]$ ničelna izogenija, tj. $[0]P = \mathcal{O}$ za vsak $P \in E$.

Lastnosti $[m]$, $\mathrm{Hom}(E_1, E_2)$ in $\mathrm{End}(E)$ povzame naslednja trditev.

Trditev 4.3.2. *[137, Trditev III.4.2].*

1. *Naj bo E/K eliptična krivulja in naj bo $m \in \mathbb{Z} - \{0\}$. Potem preslikava $[m]$ ni konstantna.*

2. *Naj bosta E_1 in E_2 eliptični krivulji. Grupa izogenij $\mathrm{Hom}(E_1, E_2)$ je $\mathbb{Z}$-modul brez torzije , tj. če za $\phi \in \mathrm{Hom}(E_1, E_2)$ obstaja tak $m \in \mathbb{Z} - \{0\}$ da je $m\phi = 0$, potem je že ϕ ničeln izogenija.*

3. *Kolobar endomorfizmov $\mathrm{End}(E)$ je kolobar s karakteristiko 0 brez deliteljev niča.*

■

Jedro preslikave $\ker([m])$ je množica vseh točk $\{P \in E(\overline{K}) :\ mP = \mathcal{O}\}$. Takim točkam pravimo torzijske točke reda m in jih bomo obravnavali v razdelku 4.5.

Primer. Naj bo E/K eliptična krivulja in $Q \in E$. Translacija za Q je preslikava

$$\begin{array}{rccc} \tau_Q : & E & \to & E, \\ & P & \mapsto & P + Q. \end{array} \tag{4.11}$$

•

Tako definirana preslikava τ_Q je očitno izomorfizem z obratno preslikavo τ_{-Q}, ni pa izogenija, za $Q \neq \mathcal{O}$. Velja pa zanjo naslednja pomembna lastnost.

Trditev 4.3.3. *Naj bo $F : E_1 \to E_2$ poljuben morfizem eliptičnih krivulj. F je možno zapisati kot produkt izogenije in translacije.*

Dokaz. Definirajmo $\phi = \tau_{-F(\mathcal{O})} \circ F$, ki je očitno izogenija, saj velja $\phi(\mathcal{O}) = \mathcal{O}$. Posledično se da F zapisati kot $F = \tau_{F(\mathcal{O})} \circ \phi$. ■

Čeprav je formulacija naslednjega izreka enostavna, je dokaz zahteven in dolg ter potrebuje teorijo deliteljev.

Izrek 4.3.4. *[137, Izrek III.4.8]. Naj bosta E_1 in E_2 eliptični krivulji in naj bo $\phi : E_1 \to E_2$ izogenija. Potem za poljubni $P, Q \in E_1$ velja $\phi(P + Q) = \phi(P) + \phi(Q)$.* ■

Posledica 4.3.5. *Naj bo $\phi : E_1 \to E_2$ neničelna izogenija. Potem je $\ker(\phi) = \phi^{-1}(\mathcal{O})$ končna podgrupa.* ■

Naslednji rezultati opišejo osnovno Galoisovo teorijo na obsegih funkcij eliptičnih krivulj.

Izrek 4.3.6. *[137, Izrek III.4.10]. Naj bo $\phi : E_1 \to E_2$ nekonstantna izogenija.*

1. *Za vsak* $Q \in E_2$, $\#\phi^{-1}(Q) = \deg_s \phi$. *Za vsak* $P \in E_1$ *je* $e_\phi(P) = \deg_i(\phi)$, *kjer je* e_ϕ *indeks ramifikacije iz definicije 3.2.12 in* $\deg_s$, $\deg_i$ *stopnji iz definicije 3.2.9.*

2. *Preslikava* $\ker(\phi) \to \mathrm{Aut}[\overline{K}(E_1)/\phi^*\overline{K}(E_2)]$, $T \mapsto \tau_T^*$ *je izomorfizem, kjer je* τ_T^* *avtomorfizem na* $\overline{K}(E_2)$, *ki ga inducira translacija* τ_T.

3. *Naj bo* ϕ *separabilna kot v definiciji 3.2.9. Potem je* ϕ *neramificiran,* $\#\ker(\phi) = \deg\phi$ *in* $\overline{K}(E_1)$ *je Galoisova razširitev* $\phi^*\overline{K}(E_2)$.

■

Posledica 4.3.7. *Naj bosta* $\phi : E_1 \to E_2$ *in* $\psi : E_1 \to E_3$ *nekonstatni izogeniji in naj bo* ϕ *separabilna. Če je* $\ker(\phi) \subset \ker(\psi)$, *potem obstaja enolična izogenija* $\lambda : E_2 \to E_3$, *za katero je* $\psi = \lambda \circ \phi$. ■

Trditev 4.3.8. *Naj bo* E *eliptična krivulja in naj bo* L *končna podgrupa* E. *Potem obstajata enolična eliptična krivulja* E' *in separabilna izogenija* $\phi : E \to E'$, *da velja* $\ker(\phi) = L$. ■

Naslednji izrek bo služil za definicijo duala izogenije.

Izrek 4.3.9. *[137, Izrek III.6.1]. Naj bo* $\phi : E_1 \to E_2$ *nekonstantna izogenija stopnje* m. *Veljata naslednji trditvi:*

1. *Obstaja enolično določena izogenija* $\hat{\phi} : E_2 \to E_1$, *ki zadošča pogoju*

$$\hat{\phi} \circ \phi = [m].$$

2. *Če na* ϕ^* *v predpisu 3.9 gledamo kot na homomofrizem grup, potem velja naslednja dekompozicija:*

$$\begin{array}{ccccccc} E_2 & \to & \mathrm{Div}^0(E_2) & \overset{\phi^*}{\to} & \mathrm{Div}^0(E_1) & \overset{\mathrm{sum}}{\to} & E_1 \\ Q & \mapsto & (Q) - (\mathcal{O}) & & \sum n_p(P) & \mapsto & \sum n_P P. \end{array}$$

■

Definicija 4.3.10. Naj bo $\phi : E_1 \to E_2$ izogenija. **Dual izogenije** k ϕ je izogenija $\hat{\phi} : E_2 \to E_1$ iz izreka 4.3.9.

4.4 Ovoji eliptičnih krivulj

Ovoji igrajo pomembno vlogo v različnih aplikacijah, ki temeljijo na parjenjih, zato si jih bomo podrobno ogledali.

Definicija 4.4.1. Naj bo E eliptična krivulja nad obsegom K. **Ovoj** krivulje E je taka eliptična krivulja E' nad obsegom K, da obstaja izomorfizem $\phi : E \to E'$ nad obsegom $\overline{K}$, za katerega velja $\phi(\mathcal{O}_E) = \mathcal{O}_{E'}$. Ovoja E' in E'' sta ekvivalentna, če med njima obstaja izomorfizem nad obsegom K. Ekvivalenčne razrede ovojev do izomorfizma nad K natančno označimo s $\mathrm{Twist}(E)$.

Primer. Naj bo K obseg s $\mathrm{char}(K) \neq 2$ in naj bo E eliptična krivulja nad K z enačbo $y^2 = x^3 + a_4x + a_6$. Naj bo $d \in K^*$ in definirajmo eliptično krivuljo $E^{(d)}$ z enačbo $y^2 = x^3 + d^2a_4x + d^3a_6$. Preslikava $\phi(x, y) = (d \cdot x, d^{3/2} \cdot y)$ je izomorfizem iz E v $E^{(d)}$, posledično je $E^{(d)}$ ovoj krivulje E v smislu definicije 4.4.1. •

Trditev 4.4.2. *Naj bo q liho praštevilo in naj bo $E : y^2 = x^3 + a_4x + a_6$ eliptična krivulja nad $\mathbb{F}_q$. Za $d \in \mathbb{F}_q^*$ veljata naslednji trditvi.*

1. *Krivulji E in ovoj $E^{(d)}$ nista izomorfni nad $\mathbb{F}_q$ natanko tedaj, ko je d prost kvadratov;*
2. *Če sta d_1 in d_2 prosta kvadratov v $\mathbb{F}_q^*$, potem sta ovoja $E^{(d_1)}$ in $E^{(d_2)}$ izomorfna nad $\mathbb{F}_q$.*

■

Po zgornji trditvi, so vsi ovoji oblike $E^{(d)}$, kjer je d prost kvadratov v $\mathbb{F}_q$ med seboj izomorfni. Ekvivalenčnemu razredu takih ovojev pravimo **kvadratni ovoji** (ang. quadratic twist).

Če je obseg $K = \mathbb{Q}$, potem obstaja neskončno mnogo neekvivalentnih ovojev $E^{(d)}$, saj lahko d teče po naravnih številih prostih kvadratov, tj. $d^2 \in \mathbb{N}$, $d \notin \mathbb{N}$. V splošnem je K razširitev K^d, kjer definiramo $K^d = \{s^d : s \in K\}$.

Trditev 4.4.3. *Naj bo E eliptična krivulja nad končnim obsegom K karakteristike* $\mathrm{char}(K) \neq 2$ *in* 3. *Če je $j(E) \neq 0$ in* 1728, *je* $\#\mathrm{Twist}(E) = 2$.

Dokaz. Naj bo E' izomorfna E nad obsegom K. Brez škode za splošnost lahko predpostavimo, da sta enačbi obeh krivulj enaki $E : y^2 = x^3+a_4x+a_6$ in $E' : y^2 = x^3+a_4'x+a_6'$. Ker sta izomorfni, velja $a_4' = u^4a_4$ in $a_6' = u^6a_6$ za nek $u \in \overline{K}^*$. Torej je $u^2 = a_6'a_4/(a_6a_4') \in K^*$. Ker je K končen obseg in $\mathrm{char}(K) \neq 2$, rezultat sledi iz dejstva, da je $[K^* : (K^*)^2] = 2$. ■

Velja celo bolj splošen rezultat zajet v naslednji trditvi.

Trditev 4.4.4. *Naj bo K končen obseg s* $\mathrm{char}(K) \neq 2, 3$ *in naj bo E eliptična krivulja nad K. Potem je*

$$\#\mathrm{Twist}(E) = \begin{cases} 2, & \text{če } j(E) \neq 0, 1728; \\ 4, & \text{če } j(E) = 1728; \\ 6, & \text{če } j(E) = 0. \end{cases}$$

■

Posplošitev zgornje trditve je naslednji izrek, katerega dokaz s pomočjo homologij najdemo v [137].

Izrek 4.4.5. *[137, Trditev X.5.4] Naj bo K obseg s karakteristiko* $\mathrm{char}(K) \neq 2, 3$ *in E eliptična krivulja nad K. Definirajmo število*

$$d = \begin{cases} 2, & \text{če } j(E) \neq 0, 1728; \\ 4, & \text{če } j(E) = 1728; \\ 6, & \text{če } j(E) = 0. \end{cases}$$

Potem je $\mathrm{Twist}(E)$ *izomorfna razširitvi* $K^*/(K^{*d})$. *Če je* $E : y^2 = x^3 + Ax + B$ *in* $D \in K^*$, *potem ima eliptična krivulja* $E_D \in \mathrm{Twist}(E)$ *glede na* $D \pmod{K^{*d}}$ *eno izmed naslednjih Weierstrassovih enačb:*

$$E_D : \begin{cases} y^2 = x^3 + D^2Ax + D^3B, & \text{če } j(E) \neq 0, 1728; \\ y^2 = x^3 + DAx, & \text{če } j(E) = 1728; \\ y^2 = x^3 + DB, & \text{če } j(E) = 0. \end{cases}$$

■

4.5 Torzijske točke

Torzijske točke igrajo pomembno vlogo v uporabi eliptičnih krivulj. V razdelku 4.6 bomo videli, da so pri eliptičnih krivuljah nad končnimi obsegi vse točke torzijske. V tem razdelku bomo najprej definirali torzijske točke, konstruirali primere 2-torzijskih in 3-torzijskih točk, nato pa bomo dokazali še nekaj splošnih lastnosti n-torzijskih točk.

Definicija 4.5.1. Naj bo E eliptična krivulja nad obsegom K in naj bo $\mathcal{O}$ točka v neskončnosti. Točka ne E je n-**torzijska točka**, če je njen red enak $n \in \mathbb{N}$. Množico n-torzijskih točk označimo z:

$$E[n] = \{P \in E(\overline{K}) : \ nP = \mathcal{O}\}.$$

Definicija 4.5.2. Torzijska podgrupa krivulje E, označena z E_{tors} je grupa vseh točk končnega reda,

$$E_{\mathrm{tors}} = \bigcup_{m=1}^{\infty} E[m].$$

Najprej si bomo ogledali lastnosti 2 in 3-torzijskih točk. Velja naslednja trditev.

Trditev 4.5.3. *Naj bo* E *eliptična krivulja nad obsegom* K.

1. *Če je karakteristika* $\mathrm{char}(K) \neq 2$, *potem je* $E[2] \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_2$.
2. *Če je karakteristika obsega* $\mathrm{char}(K) = 2$, *potem je* $E[2] \simeq 0$ *ali* $E[2] \simeq \mathbb{Z}_2$.
3. *Če je karakteristika obsega* $\mathrm{char}(K) \neq 3$, *potem je* $E[3] \simeq \mathbb{Z}_3 \oplus \mathbb{Z}_3$.
4. *Če je karakteristika obsega* $\mathrm{char}(K) = 3$, *potem je* $E[3] \simeq \mathbb{Z}_3$.

Dokaz.

1. Ker $\mathrm{char}(K) \neq 2$, je Weierstrassovo enačbo možno zapisati v obliki:

   $$E : \ y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6.$$

   Ker smo v algebraično zaprtem obsegu $\overline{K}$, lahko desno stran enačbe razstavimo

   $$E : \ y^2 = (x - e_1)(x - e_2)(x - e_3),$$

   kjer so $e_1, e_2, e_3 \in \overline{K}$. Točka P na krivulji zadošča pogoju $2P = \mathcal{O}$ natanko tedaj, ko tangenta na P poteka skozi $\mathcal{O}$. To pomeni, da je tangenta vzporedna z osjo y (glej sliko 4.2) in

   $$E[2] = \{\mathcal{O}, (e_1, 0), (e_2, 0), (e_3, 0)\}.$$

   Opazimo, da je $E[2]$ kot grupa izomorfna $\mathbb{Z}_2 \oplus \mathbb{Z}_2$.

2. Če je $\mathrm{char}(K) = 2$ imamo za Weierstrassovo enačbo dve možnosti:

$$\begin{aligned} E: &\quad y^2 + xy + a_2x^2 + a_6 = 0, &\quad a_6 \neq 0,\\ E: &\quad y^2 + a_3y + x^3 + a_4x + a_6 = 0, &\quad a_3 \neq 0. \end{aligned}$$

Vrednosti a_6 in a_3 sta različni od nič, sicer bi bila E singularna. Če ima P red 2, potem je tangenta na P navpična premica, kar v posebnem pomeni, da je njen delni odvod $\partial/\partial y$ enak 0. V prvi enačbi to pomeni, da je $x = 0$ in edina točka reda 2 je oblike $(0, \sqrt{a_6})$. Zato je $E[2] = \{\mathcal{O}, (0, \sqrt{a_6})\} \simeq \mathbb{Z}_2$. V drugi enačbi pa mora biti $a_3 = 0$. Zaradi singularnosti smo predpostavili $a_3 \neq 0$, zato je edina točka reda 2 enaka $\mathcal{O}$. Dokazali smo, da je v drugi enačbi $E[2] = \{\mathcal{O}\} \simeq 0$.

3. Najprej si oglejmo primer, ko je $\mathrm{char}(K) \neq 2, 3$. V tem primeru lahko Weierstrassovo enačbo zapišemo v obliki

$$E:\ y^2 = x^3 + Ax + B.$$

Točka P ima red 3 natanko tedaj, ko je $2P = -P$. To pomeni, da sta x koordinati točk $2P$ in P enaki, y koordinati pa sta različni. Če uporabimo eksplicitna pravila seštevanja iz trditve 4.2.4, dobimo naslednjo zvezo

$$m^2 - 2x = x, \quad \text{kjer je} \quad m = \frac{3x^2 + A}{2y}.$$

Če upoštevamo Weierstrassovo enačbo krivulje, dobimo

$$3x^4 + 6Ax^2 + 12Bx - A^2 = 0.$$

Diskriminanta tega polinoma je $-6912(4A^3 + 27B^2) \neq 0$, zato polinom nima večkratnih ničel. Tako obstajajo 4 različne vrednosti za koordinato x in vsaka vrednost x nam da dve vrednosti y. Skupaj dobimo 8 točk reda 2. Ker je tudi $\mathcal{O}$ reda 3, je $E[3] \simeq \mathbb{Z}_3 \oplus \mathbb{Z}_3$.

Preostane nam primer ko je $\mathrm{char}(K) = 2$. Enako kot v točki 2. imamo za Weierstrassovo enačbo dve možnosti:

$$\begin{aligned} E: &\quad y^2 + xy + a_2x^2 + a_6 = 0, &\quad a_6 \neq 0,\\ E: &\quad y^2 + a_3y + x^3 + a_4x + a_6 = 0, &\quad a_3 \neq 0. \end{aligned}$$

Pri prvi s pomočjo pravil za seštevanje in dejstva $2P = -P$ dobimo naslednjo enačbo za x koordinato:

$$x^4 + x^3 + a_6 = 0.$$

Diskriminanta tega polinoma je $-27a_6^2$, zato ima polinom 4 ničle. Za vsak x dobimo dve vrednosti y, tako imamo 8 različnih točk reda 3, ki skupaj s točko $\mathcal{O}$ tvorijo grupo $E[3] \simeq \mathbb{Z}_3 \oplus \mathbb{Z}_3$. Za drugo možnost Weierstrassove enačbe podobno, le da tu upoštevamo $a_3 \neq 0$.

4. Naj bo $\mathrm{char}(K) = 3$. Brez škode za splošnost lahko predpostavimo, da ima krivulja E Weierstrassovo enačbo oblike

$$y^2 = x^3 + a_2x^2 + a_4x + a_6.$$

Podobno kot zgoraj, tudi tu velja, da morata biti x koordinati točk $2P$ in P enaki. Iz eksplicitnih formul dobimo naslednjo enačbo:

$$a_2x^3 + a_2a_6 - a_4^2 = 0.$$

Če bi veljalo $a_2 = a_4 = 0$, bi imeli večkratne korene. Iz $a_2 = 0$ sledi $-a_4^2 = 0$, kar smo že izključili, zato v tem primeru ni nobene netrivialne točke reda 3 in $E[3] = \{\mathcal{O}\}$. Če pa je $a_2 \neq 0$, se enačba poenostavi v obliko $a_2(x^3 + a) = 0$, ki ima eno trojno ničlo v karakteristiki 3. Posledično je na voljo ena vrednost za x in 2 pripadajoči vrednosti za y, kar nam da dve točki reda 3. Skupaj s točko $\mathcal{O}$ je $E[3] \simeq \mathbb{Z}_3$.

■

Za n-torzijsko grupo $E[n]$ pri poljubnem n pa velja naslednji izrek, ki ga ne bomo dokazali. Dokaz je na voljo v [152] ali [137].

Izrek 4.5.4. *Naj bo E eliptična krivulja nad obsegom K in naj bo $n \in \mathbb{N}$. Če karakteristika obsega K ne deli števila n ali pa je* $\mathrm{char}(K) = 0$, *potem je*

$$E[n] \simeq \mathbb{Z}_n \oplus \mathbb{Z}_n.$$

Če pa $\mathrm{char}(K) = p > 0$ *deli* n, $n = p^r n'$ *za* $r > 0$ *in* $p \nmid n'$, *potem je*

$$E[n] \simeq \mathbb{Z}_{n'} \oplus \mathbb{Z}_{n'}$$

ali

$$E[n] \simeq \mathbb{Z}_n \oplus \mathbb{Z}_{n'}.$$

■

Naslednjo trditev bomo potrebovali v poglavju o parjenjih. Dokaže se jo s pomočjo polinomov z deljenjem (ang. division polynomials).

Trditev 4.5.5. *[152, Trditev 9.34]. Naj bo E eliptična krivulja nad obsegom K. Naj bo n naravno število, ki ni deljivo s karakteristiko obsega in naj ima funkcija $f \in \overline{K}(E)$ lastnost $f(P + T) = f(P)$ za vsak $P \in E(\overline{K})$ in vsak $T \in E[n]$. Enako kot v definiciji 3.2.3 pišemo, da je slika pola $f(P) = \infty$. Potem obstaja taka funkcija h na krivulji E, da je $f(P) = h(nP)$ za vsak $P \in E(\overline{K})$.* ■

4.6 Eliptične krivulje nad končnimi obsegi

V tem razdelku si bomo ogledali za kriptografijo najbolj zanimiv scenarij in sicer eliptične krivulje definirane nad končnimi obsegi. Že v razdelku 4.5 o torzijskih točkah smo omenili, da ima eliptična krivulja nad končnim obsegom končno točk, kar pomeni, da je tudi kot grupa končna.

V nadaljevanju bomo za končni obseg vedno vzeli obseg $\mathbb{F}_q$, kjer je q potenca praštevila, torej oblike $q = p^n$ za neko praštevilo p in $n \in \mathbb{N}$.

Izrek 4.6.1. *Naj bo E eliptična krivulja nad končnim obsegom $\mathbb{F}_q$. Potem velja*

$$E(\mathbb{F}_q) \simeq \mathbb{Z}_n$$

ali

$$E(\mathbb{F}_q) \simeq \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2},$$

za neko naravno število n ali za naravni števili n_1, n_2, kjer n_1 deli n_2.

Dokaz. Osnovni izrek iz teorije grup [150], nam pove, da je vsaka končna Abelova grupa izomorfna direktni vsoti cikličnih grup

$$\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_r},$$

kjer $n_i \mid n_{i+1}$ za $i \geq 1$. Za vsak i ima grupa $\mathbb{Z}_{n_i}$ n_1 elementov, katerih redi delijo n_1, in $E(\mathbb{F}_q)$ ima n_1^r točk, katerih redi delijo n_1. Po izreku 4.5.4 pa je takih elementov kvečjemu n_1^2, posledično je $r \leq 2$. ■

Naravno vprašanje je oceniti moč grupe $E(\mathbb{F}_q)$. Ker za vsako vrednost koordinate x dobimo maksimalno 2 vrednosti za koordinato y, je groba ocena za zgornjo mejo $2q + 1$. Ker pa je naključno izbrana krivulja malo verjetno rešljiva v obsegu K, bi za dejansko vrednost pričakovali približno q. Dejansko oceno pa nam pove naslednji izrek.

Izrek 4.6.2. *(Hassejev izrek.) Naj bo E eliptična krivulja nad končnim obsegom $\mathbb{F}_q$. Potem velja:*

$$\mid q + 1 - \#E(\mathbb{F}_q) \mid \leq 2\sqrt{q}. \tag{4.12}$$

Skica dokaza. Celoten dokaz izreka je dolg in zahteven, zato bomo samo skicirali glavne korake. Izberimo si Weierstrassovo enačbo s koeficienti v obsegu K. Naj bo

$$\begin{array}{rccc} \phi: & E & \to & E, \\ & (x,y) & \mapsto & (x^q, y^q) \end{array}$$

q-ti Frobeniusov morfizem iz definicije 3.2.15. Za točko $P \in E(\overline{K})$ velja, da je $P \in E(K)$ natanko tedaj, ko je $\phi(P) = P$ [137, poglavje III]. Torej je $E(K) = \ker(1 - \phi)$ in $\#E(K) = \#\ker(1 - \phi) = \deg(1 - \phi)$ [137, poglavje III]. Opazimo, da je deg na $\mathrm{End}(E)$ pozitivno definitna kvadratna forma [137, poglavje III] in po trditvi 3.2.16 velja $\deg \phi = q$. Ker za pozitivno definitno kvadratno formo $d : A \to \mathbb{Z}$, kjer je A Abelova grupa, za vsak $\phi, \psi \in A$ velja $\mid d(\psi - \phi) - d(\phi) - d(\psi) \mid \leq 2\sqrt{d(\phi)d(\psi)}$ [137, poglavje V], izrek sledi. ■

Zdaj ko smo spoznali glavne omejitve grupe točk na eliptični krivulji, nas zanima, kakšne so dejanske te grupe. Odgovor je v naslednjih dveh izrek, katerih dokaza najdemo v [125, 151].

Izrek 4.6.3. *Naj bo $q = p^n$ potenca praštevila p in naj števili N in t zadoščata zvezi $N = q + 1 - t$. Potem obstaja taka eliptična krivulja E definirana nad obsegom $\mathbb{F}_q$, da je $\#E(\mathbb{F}_q) = N$ natanko tedaj, ko je $\mid t \mid \leq 2\sqrt{q}$ in t zadošča enemu od naslednjih pogojev:*

1. $\gcd(t, p) = 1$;
2. *n je sodo in $t = \pm 2\sqrt{q}$;*

3. *n je sodo, $p \not\equiv 1 \pmod 3$ in $t = \pm\sqrt{q}$;*

4. *n je liho, $p = 2$ ali $p = 3$ in $t = \pm p^{(n+1)/2}$;*

5. *n je sodo, $p \not\equiv 1 \pmod 4$ in $t = 0$;*

6. *n je liho in $t = 0$.*

■

Vrednosti t v izreku 4.6.3 pravimo tudi **Frobeniusova sled** krivulje.

Izrek 4.6.4. *Naj bo N celo število, ki je red grupe točk eliptične krivulje nad končnim obsegom $\mathbb{F}_q$ kot v izreku 4.6.3. Zapišimo $N = p^e n_1 n_2$, kjer $p \nmid n_1 n_2$ in $n_1 \mid n_2$ (n_1 je lahko tudi 1). Potem obstaja taka eliptična krivulja E nad obsegom $\mathbb{F}_q$, za katero je*

$$E(\mathbb{F}_q) \simeq \mathbb{Z}_{p^e} \oplus \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$$

natanko tedaj, ko velja

1. *$n_1 \mid q - 1$ v točkah 1., 3., 4., 5., 6. izreka 4.6.3;*

2. *$n_1 = n_2$ v točki 2. izreka 4.6.3.*

■

Preden nadaljujemo z opisom lastnosti eliptičnih krivulj nad končnimi obsegi, si oglejmo še nekaj lastnosti Frobeniusovega endomorfizma na eliptičnih krivuljah nad končnimi obsegi.

V 3.2.15 smo definirali splošen Frobeniusov morfizem med krivuljami. **Frobeniusova preslikava** za obseg $\mathbb{F}_q$ je definirana kot [93]:

$$\begin{array}{rccc} \phi_q : & \overline{\mathbb{F}}_q & \to & \overline{\mathbb{F}}_q, \\ & x & \mapsto & x^q. \end{array}$$

Na eliptični krivulji Frobeniusova preslikava deluje kot $\phi_q(x, y) = (x^q, y^q)$, v posebnem je $\phi_q(\mathcal{O}) = \mathcal{O}$. Naslednja lema opisuje osnovne lastnosti tako definirane preslikave.

Lema 4.6.5. *Naj bo E eliptična krivulja definirana nad obsegom $\mathbb{F}_q$ in naj bo $(x, y) \in E(\overline{\mathbb{F}}_q)$.*

1. *$\phi_q(x, y) \in E(\overline{\mathbb{F}}_q)$.*

2. *$(x, y) \in E(\mathbb{F}_q)$ natanko tedaj, ko je $\phi_q(x, y) = (x, y)$.*

3. *ϕ_q je endomorfizem krivulje E stopnje q in ni separabilen.*

4. *Za poljuben $n \in \mathbb{N}$ velja:*

   (a) *$\ker(\phi_q^n - 1) = E(\mathbb{F}_q)$;*

   (b) *$\phi_q^n - 1$ je separabilen endomorfizem in $\#E(\mathbb{F}_{q^n}) = \deg(\phi_q^n - 1)$.*

Dokaz.

1. Naj bo E podana z enačbo $E: \ y^2 + a_1xy + a_3y = x^2 + a_2x^2 + a_4x + a_6$, kjer so $a_i \in \mathbb{F}_q$. Kot smo definirali v razdelku 3.2.2, je $E^{(q)}: \ (y^q)^2 + a_1(x^qy^q) + a_3(y^q) = (x^q)^3 + a_2(x^q)^2 + a_4(x^q) + a_6$, saj v $\mathbb{F}_q$ velja $(a+b)^q = a^q + b^q$ in $a^q = a$. Iz zgornje enačbe vidimo, da točka (x^q, y^q) leži na E.

2. Za Frobeniusovo preslikavo ϕ_q velja, da je $x \in \mathbb{F}_q$ natanko tedaj, ko je $\phi_q(x) = x$ [93]. Sledi
$$\begin{aligned}(x,y) \in E(\mathbb{F}_q) &\Leftrightarrow x, y \in \mathbb{F}_q \\ &\Leftrightarrow \phi_q(x) = x, \ \phi_q(y) = y \\ &\Leftrightarrow \phi_q(x,y) = (x,y).\end{aligned}$$

3. Dokaz sledi iz trditve 3.2.16.

   (a) Ker je ϕ_q endomorfizem na E, so endomofizmi tudi $\phi_q^n = \underbrace{\phi_q \circ \phi_q \circ \ldots \circ \phi_q}_{n \in \mathbb{N}}$, prav tako je endomorfizem tudi $\phi_q^n - 1$. Dokaz sledi potem iz točke 2.

   (b) Sledi iz posledice 3.2.17.

■

Iz leme 4.6.5 izpeljemo naslednji izrek.

Izrek 4.6.6. *[152, Izrek 4.10]. Naj bo E eliptična krivulja definirana nad obsegom $\mathbb{F}_q$. Naj bo $a = q + 1 - \#E(\mathbb{F}_q) = q + 1 - \deg(\phi_q - 1)$. Potem je*

$$\phi_q^2 + a\phi_q + q = 0,$$

kot endomorfizem krivulje E. Poleg tega a zadošča enakosti

$$a \equiv \mathrm{Sled}((\phi_q)_m) \pmod{m},$$

za vsak m tuj k q, kjer je $(\phi_q)_m$ matrika, ki jo inducira ϕ_q in opisuje delovanje ϕ_q na $E[m]$. Povedano drugače, za nek $(x,y) \in E(\overline{\mathbb{F}}_q)$ velja

$$\left(x^{q^2}, x^{q^2}\right) - a(x^q, y^q) + q(x,y) = \mathcal{O}.$$

■

Definicija 4.6.7. Polinom $X^2 - aX + q$ imenujemo tudi **Frobeniusov karakteristični polinom**.

Zdaj lahko izračunamo red grupe točk na eliptični krivulji.

Izrek 4.6.8. *[152, Izrek 4.12]. Naj bo $\#E(\mathbb{F}_q) = q+1-a$ in $X^2-aX+q = (X-\alpha)(X-\beta)$. Potem za vsak $n \in \mathbb{N}$ velja*

$$\#E(\mathbb{F}_{q^n}) = q^n + 1 - (\alpha^n + \beta^n).$$

■

Za naslednji rezultat najprej definirajmo Legendreov simbol. Osnovni Legendreov simbol za liho praštevilo p je definiran kot:

$$\left(\frac{x}{p}\right) = \begin{cases} +1, & \text{če ima } t^2 \equiv x \pmod{p} \text{ rešitev } t \not\equiv 0 \pmod{p}; \\ -1, & \text{če } t^2 \equiv x \pmod{p} \text{ nima rešitve } t; \\ 0, & \text{če je } x \equiv 0 \pmod{p}. \end{cases} \tag{4.13}$$

To lahko posplošimo za poljuben končen obseg $\mathbb{F}_q$, kjer je q potenca lihega praštevila:

$$\left(\frac{x}{\mathbb{F}_q}\right) = \begin{cases} +1, & \text{če ima } t^2 = x \text{ rešitev } t \in \mathbb{F}_q^*; \\ -1, & \text{če } t^2 = x \text{ nima rešitve } t \in \mathbb{F}_q; \\ 0, & \text{če je } x = 0. \end{cases} \tag{4.14}$$

Izrek 4.6.9. *[152, Izrek 4.14.]. Naj bo E eliptična krivulja definirana z enačbo $E: y^2 = x^3 + Ax + B$ nad obsegom $\mathbb{F}_q$. Potem velja*

$$\#E(\mathbb{F}_q) = q + 1 + \sum_{x \in \mathbb{F}_q} \left(\frac{x^3 + Ax + B}{\mathbb{F}_q}\right).$$

■

Naslednje trditve nam bodo opisale rede posameznih točk. Če najdemo dovolj točk z določenim redom, lahko izračunamo celoten red grupe.

Trditev 4.6.10. *[152, Trditev 4.16]. Naj bo E eliptična krivulja nad obsegom $\mathbb{F}_q$ in naj bo*

$$E(\mathbb{F}_q) \simeq \mathbb{Z}_n \oplus \mathbb{Z}_n$$

za neko naravno število n. Potem velja $q = n^2 + 1$ ali $q = n^2 \pm n + 1$ ali $q = (n \pm 1)^2$. ■

Večina vrednosti q ne ustreza nobeni možnosti v trditvi 4.6.10 pa tudi pri naštetih oblikah q večina krivulj nima reda n^2, zato je tak primer redek. Bolj verjetno je, da imajo po Hassejevem izreku 4.6.2 eliptične krivulje nad $\mathbb{F}_q$ za večino vrednosti q red večji od $4\sqrt{q}$. Če na E najdemo dovolj točk takega reda, lahko ugotovimo $\#E(\mathbb{F}_q)$.

Trditev 4.6.11. *[152, Trditev 4.18]. Naj bo $p > 229$ praštevilo in naj bo E eliptična krivulja nad $\mathbb{F}_p$. Potem obstaja točka P na E ali njenem kvadratnem ovoju E' reda r_P, tako da v intervalu $(p + 1 - 2\sqrt{p}, p + 1 + 2\sqrt{p})$ leži samo en večkratnik r_p.* ■

Če pa je recimo $E(\mathbb{F}_q) \simeq \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$ kjer $n_1 \mid n_2$, potem lahko iz informacij o n_2 sklepamo na strukturo grupe.

Trditev 4.6.12. *[152, trditev 4.19] Naj bo E eliptična krivulja nad obsegom $\mathbb{F}_q$ in naj bo $E(\mathbb{F}_q) \simeq \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$, kjer $n_1 \mid n_2$. Izberimo q različen od naslednjih vrednosti: 3, 4, 5, 7, 9, 11, 13, 17, 19, 23, 25, 27, 29, 31, 37, 43, 61, 73, 181, 331, 547. Potem n_2 enolično določa n_1.* ■

Red posamezne točke lahko izračunamo z algoritmom mali korak-veliki korak [152, poglavje 4]. Najboljši algoritmi za računanje števila točk na eliptični krivulji temeljijo na Schoofovem algoritmu [131] in njegovih izpeljankah [17, 132] ali pa uporabljajo aritmetično-geometrijsko povprečje (ang. Arithmetic-Geometric-Mean - AGM) [103, 35].

Naslednji izrek nam zagotovi povezavo med p-torzijsko grupo $E[p]$ in $\mathrm{End}(E)$. Uporaben bo tudi v naslednjem razdelku, ko bomo definirali supersingularne krivulje.

Izrek 4.6.13. *[137, Izrek V.3.1]. Naj bo K popoln obseg (definiran v A.2.8) karakteristike p in naj bo E/K eliptična krivulja. Za vsako naravno število r označimo zaporedoma*

$$\phi_r : E \to E^{(p^r)} \quad in \quad \hat{\phi}_r : E^{(p^r)} \to E$$

Frobeniusov p^r endomorfizem in njegov dual izogenije (iz izreka 4.3.9).

1. *Naslednje trditve so ekvivalentne:*
   (a) $E[p^r] = \{\mathcal{O}\}$;
   (b) $\hat{\phi}_r$ *je (čisto) neseparabilen za vsak* $r \geq 1$;
   (c) *Preslikava* $[p] : E \to E$ *je čisto neseparabilna in* $j(E) \in \mathbb{F}_{p^2}$;
   (d) $\mathrm{End}(E)$ *je red v algebri kvaternionov (definirani v A.1.4).*
2. *Če trditvam v točki 1. ni zadoščeno, potem je*

$$E[p^r] = \mathbb{Z}/p^r\mathbb{Z}, \quad za\ vsak \quad r \in \mathbb{N},$$

in če je $j(E) \in \overline{\mathbb{F}}_p$, *potem je* $\mathrm{End}(E)$ *red v imaginarnem kvadratnem obsegu.*

■

Na koncu si oglejmo še eno endomorfizem na E, ki bo uporaben pri parjenjih.

Definicija 4.6.14. Naj bo $P = (x, y) \in E(\mathbb{F}_{q^k})$. **Sled** je preslikava, definirana po točkah kot

$$\mathrm{Tr}(P) = \sum_{\sigma \in Gal(\mathbb{F}_{q^k}/\mathbb{F}_q)} \sigma(P) = \sum_{i=0}^{k-1} (x^{q^i}, y^{q^i}),$$

kjer je vsota seštevanje v grupi točk na eliptični krivulji E.

4.7 Vključitvena stopnja

Pomemben pojem, ki ga bomo v potrebovali pri konstrukciji krivulj, je vključitvena stopnja eliptičnih krivulj.

Definicija 4.7.1. E eliptična krivulja definirana nad obsegom K naj ima K-racionalno točko reda r, kjer je r tuj k $\mathrm{char}(K)$. **Vključitvena stopnja** krivulje E glede na r je stopnja razširitve $[K(\mu_r) : K]$, kjer je μ_r grupa r-tih korenov enote.

Pri določenih pogojih ima vključitvena stopnja več ekvivalentnih pomenov. Le te zajema naslednja trditev, ki je posledica definicije in lastnosti μ_r opisanih v razdelku A.2.6.

Trditev 4.7.2. *Naj bo r naravno število, ki deli $\#E(\mathbb{F}_q)$ in je tuje k q. Potem so naslednji trije pogoji ekvivalentni:*

1. *E ima vključitveno stopnjo k glede na r;*
2. *k je tako najmanjše celo število, da r deli $q^k - 1$;*
3. *$q \in (\mathbb{Z}/r\mathbb{Z})^*$ je reda k.*

■

Opomba: Razširjenemu obsegu $\mathbb{F}_q(\mu_r)$ pravimo tudi **minimalni vključitveni obseg** krivulje E.

4.8 Supersingularne in navadne krivulje

V tem razdelku bomo definirali supersingularne krivulje. Supersingularne krivulje imajo posebne lastnosti zaradi katerih so uporabne v protokolih s parjenji.

Ekvivalentnih definicij supersingularnih krivulj je več, najprej navedimo definicijo, ki temelji na izreku 4.6.13.

Definicija 4.8.1. Če krivulja E zadošča eni izmed lastnosti v točki 1. izreka 4.6.13, potem je E **supersingularna**, sicer je E **navadna**.

Za praštevilske obsege, sta zgornja in naslednja definicija ekvivalentni.

Definicija 4.8.2. Naj bo q potenca praštevila in E eliptična krivulja nad $\mathbb{F}_q$. Definirajmo **Frobeniusovo sled** krivulje $E/\mathbb{F}_q$ kot $t = q+1-\#E(\mathbb{F}_q)$. Hassejev izrek 4.6.2 nam pove, da je $|t| \leq 2\sqrt{q}$. Če sta t in q tuji, potem za eliptično krivuljo pravimo da je **navadna**, drugače je **supersingularna**.

Največkrat pa bomo uporabljali naslednjo definicijo, ki povzame glavne pogoje, pri katerih je krivulja supersingularna.

Definicija 4.8.3. Naj bo E eliptična krivulja nad $\mathbb{F}_q$, kjer je q potenca praštevila p. E je **supersingularna**, če je izpolnjen kateri izmed naslednjih pogojev:

1. $\#E(\mathbb{F}_q) \equiv 1 \pmod{p}$, oziroma ekvivalentno $\#E(\mathbb{F}_q) = q + 1 - t$, kjer $p|t$;
2. E nima točk reda p nad obsegom $\overline{\mathbb{F}}_q$;
3. End(E) je nekomutativen, torej je red v algebri kvaternionov.

S pomočjo Waterhousovega izreka [151] je mogoče dokazati, da za vsako praštevilo p in $m \in \mathbb{N}$ obstaja supersingularna eliptična krivulja nad obsegom $\mathbb{F}_{p^m}$. Naslednji izrek pa nam pove koliko je supersingularnih krivulj.

Izrek 4.8.4. *[137, Izrek V.4.1]. Naj bo K obseg karakteristike $p > 2$. Do izomorfizma natančno obstaja natanko $\lfloor p/12 \rfloor + \epsilon_p$ supersingularnih krivulj nad K, kjer je*

$$\epsilon_p = \begin{cases} 0, & \text{če je } p \geq 5 \text{ in } p \equiv 1 \pmod{12}; \\ 1, & \text{če je } p \geq 5 \text{ in } p \equiv 5 \pmod{12} \text{ ali } p \equiv 7 \pmod{12}; \\ 2, & \text{če je } p \geq 5 \text{ in } p \equiv 11 \pmod{12}; \\ 3, & \text{če je } p = 3. \end{cases}$$

■

Supersingularne krivulje imajo omejen nabor vrednosti za vključitveno stopnjo, kar nam pove naslednji izrek.

Izrek 4.8.5. *V tabeli so zajete vse možne vrednosti vključitvenih stopenj skupaj s strukturo grupe supersingularnih krivulj nad $\mathbb{F}_q$.*

k	q	$\#E(\mathbb{F}_q)$	*Grupa v* $E(\mathbb{F}_{q^k})$
1	p^{2b}	$q \pm 2\sqrt{q} + 1$	$(\mathbb{Z}/(\sqrt{q} \pm 1)\mathbb{Z})^2$
2	p^a, *a liho, ali a sodo in* $p \not\equiv 1 \pmod{4}$	$q + 1$	$(\mathbb{Z}/(q+1)\mathbb{Z})^2$
3	p^a, $p \not\equiv 1 \pmod{3}$, *a sodo*	$q + \sqrt{q} + 1$	$(\mathbb{Z}/(q^{3/2} - 1)\mathbb{Z})^2$
3	p^a, $p \not\equiv 1 \pmod{3}$, *a sodo*	$q - \sqrt{q} + 1$	$(\mathbb{Z}/(q^{3/2} + 1)\mathbb{Z})^2$
4	2^{2b+1}	$q \pm \sqrt{2q} + 1$	$(\mathbb{Z}/(q^2 + 1)\mathbb{Z})^2$
6	3^{3b+1}	$q \pm \sqrt{3q} + 1$	$(\mathbb{Z}/(q^3 + 1)\mathbb{Z})^2$

(4.15)

Dokaz. Naj bo $q = p^a$. Ker je E supersingularna, je število točko krivulje E nad obsegom $\mathbb{F}_q$ enako $q + 1 - t$, kjer t zadošča enemu od pogojev 2. - 6. v izreku 4.6.3.

Karakteristični polinom q-tega Frobeniusovega endomorfizma ϕ krivulje E nad $\mathbb{F}_q$ je $P(X) = X^2 - tX + q$. Nad $\mathbb{C}$ je $P(X) = (X - \alpha)(X - \overline{\alpha})$ in karakteristični polinom q^k-tega Frobeniusovega endomorfizma je enak $(X - \alpha^k)(X - \overline{\alpha}^k)$. V posebnem je $\#E(\mathbb{F}_{q^k}) = q^k + 1 - \alpha^k - \overline{\alpha}k$. Če je karakteristični polinom q^k-tega Frobeniusovega endomorfizma enak $(X - \alpha^k)^2$ za $\alpha^k \in \mathbb{Z}$, je $E(\mathbb{F}_{q^k})$ izomorfna $(\mathbb{Z}/|1 - \alpha^k|\mathbb{Z})^2$ po [140, trditev 2]. Zdaj bomo preverili vse možnosti za t.

1. Če je $t = \pm 2\sqrt{q}$, je q kvadrat in $P(X) = (X \pm \sqrt{q})^2$. Ker velja $(\sqrt{q} + 1)(\sqrt{q} - 1) = (q - 1)$ je vključitvena stopnja $k = 1$.

2. Če je $t = \pm\sqrt{q}$, je q kvadrat in $\#E(\mathbb{F}_q) = (q \pm \sqrt{q} + 1)$. Iz $(q \pm \sqrt{q} + 1)(\sqrt{q} \mp 1) = q^{3/2} \mp 1$ in $(q^{3/2} - 1)(q^{3/2} + 1) = (q^3 - 1)$ sklepamo, da je $k = 3$.

3. Če je $t = \pm p^{(a+1)/2}$ ločimo dva podprimera:

   - Pri $p = 2$ je $\#E(\mathbb{F}_q) = (2^a \pm 2^{(a+1)/2} + 1)$. Karakteristični polinom Frobeniusovega endomorfizma je $X^2 \pm 2^{(a+1)/2}X + 2^a$ s korenoma

   $$\alpha = 2^{a/2}\left(\frac{1 - i}{\sqrt{2}}\right) \quad \text{in} \quad \overline{\alpha} = 2^{a/2}\left(\frac{-1 + i}{\sqrt{2}}\right).$$

   Velja $\alpha^4 = \overline{\alpha}^4 = -2^{2a}$ in tako je karakteristični polinom Frobeniusovega endomorfizma krivulje E nad $\mathbb{F}_{q^4}$ enak $(X + q^2)^2$. Posledično je $(1 + q^2)P = \mathcal{O}$ za vsako točko $P \in E(\mathbb{F}_{q^4})$ ter $E(\mathbb{F}_{q^4}) \simeq (\mathbb{Z}/(q^2 + 1)\mathbb{Z})^2$. Ker $(q + \sqrt{2q} + 1)(q - \sqrt{2q} + 1) = (q^2 + 1)$ deli $(q^4 - 1)$, je $k = 4$.

   - Pri $p = 3$ je $\#E(\mathbb{F}_q) = (q \pm \sqrt{3q} + 1)$ in karakteristični polinom Frobeniusovega endomorfizma ima korena

   $$\alpha = 3^{a/2}\left(\frac{\sqrt{3} - i}{2}\right) \quad \text{in} \quad \overline{\alpha} = 3^{a/2}\left(\frac{-\sqrt{3} + i}{2}\right).$$

   Iz $\alpha^6 = \overline{\alpha}^6 = -3^{3a}$ sklepamo, da je karakteristični polinom Frobeniusovega endomorfizma krivulje E nad $\mathbb{F}_{q^6}$ enak $(X + q^3)^2$ Ker velja $(q + 1)(q + \sqrt{3q} + 1)(q - \sqrt{3q} + 1) = (q + 1)(q^2 - 1 + 1) = (q^3 + 1)$, sklepamo, da je $k = 6$.

4. Če je $t = 0$, je $\#E(\mathbb{F}_q) = (q + 1)$ in n deli $(q - 1)(q + 1) = (q^2 - 1)$. Posledično je $k = 2$.

■

Naslednji rezultat so prvi dokazali Menezes, Okamoto in Vanstone [102] pred izrekom 4.8.5.

Posledica 4.8.6. *Supersingularne krivulje imajo vključitveno stopnjo $k \leq 6$.* ■

Posledica 4.8.7. *Naj bo $p \geq 5$ praštevilo in naj bo E eliptična krivulja nad $\mathbb{F}_p$. Potem je E supersingularna natanko tedaj, ko je Frobeniusova sled $t = 0$, kar je ekvivalentno $\#E(\mathbb{F}_p) = p + 1$.*

Dokaz. Če je $t = 0$, potem je E supersingularna po definiciji 4.8.3. Obratno, naj bo E supersingularna in $t \neq 0$. Potem iz $t \equiv 0 \pmod{p}$ sledi, da je $|t| \geq p$. Po Hassejevem izreku 4.6.2 je $|t| \leq 2\sqrt{p}$. Od tod sklepamo $p \leq 2\sqrt{p}$, kar pomeni $p \leq 4$. ■

Ena izmed prednosti supersingularnih krivulj je v hitrejšem računanju kP, kjer je k naravno število in P točka na krivulji. Prihranek pri računanju gre na račun zamenjave seštevanja točk na krivulji z računanjem v končnem obsegu, ki je ponavadi hitrejše [152, poglavje 4].

Primer. Navedimo tri zglede supersingularnih krivulj.

- Naj bo $p \equiv 2 \pmod{3}$ praštevilo in naj bo $a_6 \in \mathbb{F}_p^*$. Eliptična krivulja podana z enačbo $E: \ y^2 = x^3 + a_6$ je supersingularna, saj ima $p + 1$ točk.

- Naj bo $p \equiv 3 \pmod{4}$ praštevilo in $a_4 \in \mathbb{F}_p^*$. Eliptična krivulja $E: \ y^2 = x^3 + a_4 x$ ima tudi $p + 1$ točk in je zato supersingularna.

- Naj bo $\mathbb{F}_q$ končni obseg s karakteristiko 2 in naj bo $F(x) \in \mathbb{F}_q[x]$ monični polinom stopnje 3. Potem je eliptična krivulja $E: \ y^2 + y = F(x)$ supersingularna. To sledi iz dejstva, da je $(x, y) \in E(\mathbb{F}_{q^n})$ natanko tedaj, ko je $(x, y+1) \in E(\mathbb{F}_{q^n})$. Posledično je $\#E(\mathbb{F}_{q^n})$ liho za vsak n. Tako ne obstaja nobena točka reda 2 na $E(\overline{\mathbb{F}}_2)$, zato je E supersingularna.

•

Izrek 4.8.8. *[67, Trditev 13.6.2] Naj bo E eliptična krivulja nad $\mathbb{F}_{p^m}$, kjer je p praštevilo. Če je E supersingularna, potem ima karakteristični polinom Frobeniusovega endomorfizma $P(X) = X^2 + tX + p^m$ nad $\mathbb{C}$ korena α_1 in α_2 z lastnostjo, da sta $\alpha_1/\sqrt{p^m}$ in $\alpha_1/\sqrt{p^m}$ korena enote.* ■

Naslednja rezultata povežeta lastnosti supersingularnih krivulj in Frobeniusovih morfizmov.

Lema 4.8.9. *Naj bo E supersingularna krivulja nad obsegom $\mathbb{F}_q$ in $P(X)$ karakteristični polinom Frobeniusovega endomorfizma. Potem v kolobarju $\mathbb{R}[x]$ vsak linearni faktor $\frac{1}{q}P(X\sqrt{q})$ deli $\Phi_m(X^2)$ za nek $m \in \{1, 2, 3, 4, 6\}$, kjer $\Phi_m(x)$ označuje m-ti ciklotomični polinom.*

Dokaz. S pomočjo izreka 4.6.3 lahko dobimo vse možnosti za karakteristični polinom $P(X) = X^2 + tX + q$ Frobeniusovega endomorfizma. Vrednost t je lahko $0, \pm\sqrt{q}$, $\pm 2\sqrt{q}$, $\pm\sqrt{2q}$ če je q potenca števila 2, ali $\pm\sqrt{3q}$ če je q potenca 3. Označimo $P(X) = (X - \alpha)(X - \beta)$. Potem sta po izreku 4.8.8 $\alpha/\sqrt{q}$ in $\beta/\sqrt{q}$ korena enote in

$$(X - \alpha/\sqrt{q})(X - \beta/\sqrt{q}) = \frac{1}{q}P(X\sqrt{q}).$$

Naj bo $Q(X) = P(X\sqrt{q})/q$. Prve tri vrednosti t dajo naslednje možnosti za $Q(X): X^2+1$, $X^2 \pm X + 1$ in $X^2 \pm 2X + 1 = (X \pm 1)^2$. Za prva dva t lema velja. Pogoj o linearnih faktorjih je potreben, saj $(X \pm 1)$ deli $\phi_1(X^2) = (X - 1)(X + 1)$, medtem ko $(X \pm 1)^2$

ne deli nobenega ciklotomičnega polinoma. Ostaneta nam še preostali dve možnosti za t. Najprej izberimo $t = \pm 2^{(m+1)/2}$ kjer je $q = 2^m$. Potem je $Q(X) = X^2 \pm \sqrt{2}X + 1$ in

$$(X^2 + \sqrt{2}X + 1)(X^2 - \sqrt{2}X + 1) = X^4 + 1 = \phi_4(X^2).$$

Podobno za $t = \pm 3^{(m+1)/2}$ kjer je $q = 3^m$ dobimo $Q(X) = X^2 \pm \sqrt{3}X + 1$ in

$$(X^2 + \sqrt{3}X + 1)(X^2 - \sqrt{3}X + 1) = X^4 - X^2 + 1 = \phi_6(X^2).$$

■

V povezavi z ovoji definiranimi v razdelku 4.4 velja naslednji izrek.

Izrek 4.8.10. *Naj bo E eliptična krivulja nad obsegom $\mathbb{F}_q$ s podgrupo praštevilskega reda $r > 3$ in vključitveno stopnjo $k > 1$ glede na r. Če ima E ovoj $E'/\mathbb{F}_q$ stopnje k in je $r > 4\sqrt{q}$, potem je E supersingularna.*

Dokaz. Po [65, izrek 3] obstaja enoličen ovoj E' stopnje k krivulje za katerega r deli $\#E'(\mathbb{F}_q)$. Iz predpostavke $r > 4\sqrt{q}$ sledi, da kvečjemu en večkratnik števila r leži v Hassejevem intervalu $[q+1-2\sqrt{q}, q+1+2\sqrt{q}]$. Ker morata biti po Hassejevem izreku 4.6.2 vrednosti $\#E(\mathbb{F}_q)$ in $\#E'(\mathbb{F}_q)$ znotraj tega intervala, mora veljati $\#E(\mathbb{F}_q) = \#E'(\mathbb{F}_q)$. Po Tateovem izreku [147] obstaja izogenija $\psi : E \to E'$ definirana nad $\mathbb{F}_q$. Iz predpostavke, da je E' ovoj krivulje E stopnje $k > 1$ sledi, da sta E in E' izomorfni nad razširitvijo obsega $\mathbb{F}_q$, nista pa izomorfni nad osnovnim obsegom $\mathbb{F}_q$. Kompozitum izogenije in izomorfizma porodi endomorfizem ψ krivulje E, ki ni definiran nad $\mathbb{F}_q$, iz česar sledi, da ne komutira s Frobeniusovim endomorfizmom krivulje E. Od tod sklepamo, da $\mathrm{End}(E)$ ni komutativen, torej mora biti E supersingularna. ■

4.9 Kompleksno množenje

V tem razdelku bomo pokazali, da je kolobar endomorfizmov eliptične krivulje E ali izomorfen $\mathbb{Z}$ ali redu imaginarnega kvadratnega obseg definiranega v A.2.31. Če je $\mathrm{End}(E)$ strogo večji od $\mathbb{Z}$ bomo rekli, da ima krivulja E kompleksno množenje (CM). Izkazalo se bo, da imajo vse krivulje nad končnimi obsegi kompleksno množenje.

4.9.1 Eliptične krivulje nad $\mathbb{C}$

Za lažjo definicijo kompleksnega množenja bomo predstavili eliptične krivulje nad $\mathbb{C}$ z mrežami. Večino lastnosti ne bomo dokazali, dokazi so na voljo v [152, poglavje 9] in [137].

Trditev 4.9.1.

1. *Eliptična krivulja $E: y^2 = 4x^3 - g_2x - g_3$ nad $\mathbb{C}$ je izomorfna $\mathbb{C}/L$, kjer je $L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ mreža v kompleksni ravnini za linearno neodvisni kompleksni števili $\omega_1, \omega_2 \in \mathbb{C}$ nad $\mathbb{R}$. Kvocient $\mathbb{C}/L$ ustreza torusu.*

2. *Naj bo E eliptična krivulja nad $\mathbb{C}$, ki jo porodi mreža L. Potem je $End(E) \simeq \{\beta \in \mathbb{C} : \beta L \subseteq L\}$.*

■

Definicija 4.9.2. Naj bo L mreža in naj bo $k \geq 3$ naravno število. Definirajmo **Eisensteinovo vrsto** kot

$$G_k = G_k(L) = \sum_{\omega \in L, \omega \neq 0} \omega^{-k}.$$

Izberimo tako mrežo $L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$, da bo $\tau = \omega_1/\omega_2$ ležal v zgornji kompleksni ravnini $\mathcal{H} = \{x + iy \in \mathbb{C} : \ y > 0\}$. Naj bo $L_\tau = \mathbb{Z}\tau + \mathbb{Z}$ mreža napeta na τ in 1. Za naravno število $k \geq 3$ definirajmo

$$G_k(\tau) = G_k(L_\tau) = \sum_{(m,n) \neq (0,0)} \frac{1}{(m\tau + n)^k}.$$

Mreža L' je **homotetična** mreži L, če obstaja tako neničelno kompleksno število λ, da je $L = \lambda L'$.

Po [152, poglavje 10] je množica homeotetnih razredov končna. Vrsta G_k konvergira in za lihe k je $G_k = 0$. Mreža L_τ je homotetična mreži L, kjer je $\lambda = \omega_2$ in $G_k(\tau) = \omega_2^k G_k(L)$.

V nadaljevanju bomo uporabljali standardne oznake v teoriji eliptičnih krivulj nad $\mathbb{C}$ in sicer:

$$\begin{aligned} g_2 = g_2(L) &= 60\, G_4, \\ g_3 = g_3(L) &= 140\, G_6, \\ \delta &= g_2^3 - 27 g_3^2, \\ j(\tau) &= 1728 \frac{g_2^3}{\delta}, \end{aligned} \tag{4.16}$$

kjer sta δ in j diskriminanta in j-invarianta eliptične krivulje $\mathbb{C}/L$. Opazimo, da sta zgornji formuli za δ in $j(\tau)$ podobni kot pri Weierstrassovih formulah (4.5). Za računanje $j(\tau)$ obstajajo eksplicitne formule, ki jih najdemo v [152, trditev 9.12, 9.13].

Izrek 4.9.3. *Naj bo E eliptična krivulja nad $\mathbb{C}$. Kolobar endomorfizmov* $\mathrm{End}(E)$ *je izomorfen ali $\mathbb{Z}$ ali redu imaginarnega kvadratnega obsega.*

Dokaz. Naj bo $L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ mreža, ki definira krivulji E. Množica

$$R = \{\beta \in \mathbb{C} : \ \beta L \subseteq L\}.$$

je zaprta za seštevanje, odštevanje in množenje, torej je kolobar. Velja tudi $\mathbb{Z} \subset R$. Izberimo $\beta \in R$, potem obstajajo taka cela števila j, k, m, n, da je $\beta\omega_1 = j\omega_1 + k\omega_2$ in $\beta\omega_2 = m\omega_1 + n\omega_2$. V matrični obliki dobimo

$$\begin{pmatrix} \beta - j & -k \\ m & \beta - n \end{pmatrix} \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} = 0.$$

Determinanta zgornje matrike je 0 in posledično velja $\beta^2 - (j+n)\beta + (jn - km) = 0$. Ker so j, k, m, n cela števila, je β algebraično celo število in leži v nekem kvadratnem obsegu K (glej dodatek A.2.5).

Ob predpostavki, da je $\beta \in \mathbb{R}$, iz $(\beta - j)\omega_1 - k\omega_2 = 0$ in dejstva, da sta ω_1 in ω_2 linearno neodvisna nad $\mathbb{R}$ sledi, $\beta = j \in \mathbb{Z}$ in $R \cap \mathbb{R} = \mathbb{Z}$.

Predpostavimo, da $R \neq \mathbb{Z}$. Izberimo $\beta \in R$ in $\beta \notin \mathbb{Z}$. Potem je β algebraično celo število v kvadratnem obsegu K. Ker $\beta \notin \mathbb{R}$, mora biti K imaginaren kvadratni obseg $K = \mathbb{Q}(\sqrt{d})$ za nek $d \in \mathbb{Z}$. Izberimo še $\beta' \notin \mathbb{Z}$ iz R. Potem tudi za β' velja $\beta' \in K' = \mathbb{Q}(\sqrt{d'})$

za nek $d' \in \mathbb{Z}$. Ker mora $\beta + \beta'$ tudi ležati v algebraičnem obsegu, je $K = K'$ in $R \subset K$. Vsi elementi v R so algebraična cela števila, zato je R vsebovan v kolobarju celih števil O_K (definiranem v A.2.5). Torej, če $R \neq \mathbb{Z}$, je R red v imaginarnem kvadratnem obsegu. ■

Definicija 4.9.4. Naj bo E eliptična krivulja nad obsegom K. Če je End(E) strogo večji od $\mathbb{Z}$, potem **ima** E **kompleksno množenje** v redu $\{\beta \in \mathbb{C} : \ \beta L \subseteq L\} \simeq \mathrm{End}(E)$.

Trditev 4.9.5. *[152, Trditev 10.3] Naj bo R red v imaginarnem kvadratnem obsegu in naj bo L mreža za katero velja $R = \mathrm{End}(\mathbb{C}/L)$. Potem obstaja tak $\gamma \in \mathbb{C}^*$, da je γL ideal v R. Obratno, če za podmnožico $L \subseteq \mathbb{C}$ in $\gamma \in \mathbb{C}^*$ velja, da je γL ideal v R, potem je L mreža in $R \subseteq \mathrm{End}(\mathbb{C}/L)$.* ■

Trditev 4.9.6. *Naj bo R red v imaginarnem kvadratnem obsegu in naj bo L taka mreža, da je $RL \subseteq L$. Potem je število $j(L)$ algebraično nad $\mathbb{Q}$.*

Dokaz. Naj bo E eliptična krivulja porojena z mrežo L. Brez škode za splošnost lahko predpostavimo, da je E podana z enačbo $y^2 = 4x^3 - g_2x - g_3$. Naj bo σ avtomorfizem obsega $\mathbb{C}$ in E^σ eliptična krivulja definirana z enačbo $y^2 = 4x^3 - \sigma(g_2)x - \sigma(g_3)$. Če je α endomorfizem na E, potem je α^σ endomorfizem na E^σ, kjer α^σ dobimo iz α tako, da σ deluje na koeficientih racionalnih funkcij, ki definirajo α. To pomeni $\mathrm{End}(E) \simeq \mathrm{End}(E^\sigma)$. Mreža ki porodi E^σ pripada eni izmed končno mnogo homotetičnih razredov mrež, ki vsebujejo R. Po definiciji je $\sigma(j(L))$ j-invarianta od E^σ. Zato ima $j(L)$ končno mnogo možnih slik glede na avtomorfizme obsega $\mathbb{C}$, kar pomeni, da je $j(L)$ algebraična nad $\mathbb{Q}$ [152, dodatek C]. ■

Posledica 4.9.7. *Naj bo K imaginarni kvadratni obseg.*

1. *Izberimo $\tau \in \mathcal{H}$. Potem ima $\mathbb{C}/(\mathbb{Z}\tau + \mathbb{Z})$ kompleksno množenje z redom v K natanko tedaj, ko je $\tau \in K$.*

2. *Če je $\tau \in \mathcal{H}$ vsebovan v K, potem je $j(\tau)$ algebraično število nad $\mathbb{Q}$.*

Dokaz.

1. Iz trditve 4.9.1 sledi, če ima $\mathbb{C}/(\mathbb{Z}\tau + \mathbb{Z})$ kompleksno množenje z redom v K, potem je $\tau \in K$. Obratno, naj bo $\tau \in K$. Potem τ zadostuje enačbi $a\tau^2 + b\tau + c = 0$ za cela števila a, b, c in $a \neq 0$. Množenje z $a\tau$ slika mrežo $L_\tau = \mathbb{Z}\tau + \mathbb{Z}$ vase: $a\tau \cdot \tau = -b\tau - c \in L_\tau$. Posledično ima $\mathbb{C}/L_\tau$ kompleksno množenje.

2. Izberimo $\tau \in K$. Naj bo R kolobar endomorfizmov krivulje $\mathbb{C}/L_\tau$. Po točki 1. je $R \neq \mathbb{Z}$, torej je R red v K in po trditvi 4.9.6 je $j(\tau)$ algebraičen nad $\mathbb{Q}$.

■

Naslednji izrek nam bo koristil pri opisu algoritma za konstrukcijo krivulj.

Izrek 4.9.8. *[17, Izrek VIII.2]. Naj bo $\tau \in \mathcal{H}$ kompleksno kvadratno število z diskriminanto $-D$, kot je v definiciji A.2.35. Število razredov reda kvadratnega obsega z diskriminanto $-D$ označimo s h_D. Potem je $j(\tau)$ algebraično število stopnje h_D in njegov minimalni polinom je podan z*

$$H_D(x) = \prod (x - j(\alpha)),$$

kjer α teče po vseh kompleksnih številih, za katere je par $(\alpha, 1)$ ničla ene izmed h_D ekvivalentnih primitivnih reduciranih form diskriminante $-D$. ■

Pokazali smo že, da je $j(\tau)$ algebraičen nad $\mathbb{Q}$, kar pomeni, da je j-invarianta koren polinoma z racionalnimi koeficienti. Velja tudi bolj splošen rezultat, ki ga opiše naslednji izrek.

Izrek 4.9.9. *[152, Izrek 10.9]. Naj bosta R red v imaginarnem kvadratnem obsegu in L mreža z lastnostjo $RL \subseteq L$. Potem je $j(\tau)$ algebraično celo število. Ekvivalentno, naj bo E eliptična krivulja nad obsegom $\mathbb{C}$ s kompleksnim množenjem. Potem je $j(E)$ algebraično celo število.* ■

Izrek 4.9.9 nam pove, da je j-invarianta koren moničnega polinoma s celoštevilskimi koeficienti.

Če je $\mathbb{Z}[\tau]$ maksimalni red nekega imaginarnega kvadratnega obsega K, potem je $H = K(j(\tau))$ razširitev obsega K stopnje h_D. Ta razširitev je maksimalna neramificirana Abelova razširitev kot v dodatku A.2.27. Galoisova grupa razširitve H nad K je izomorfna grupi razredov obsega K, poleg tega H zadošča definiciji Hilbertovih obsegov razredov.

V nadaljevanju bomo predpostavili, da je $\mathbb{Z}[\tau]$ maksimalen red v nekem imaginarnem kvadratnem obsegu. Naj $-D$ označuje diskriminanto, torej je $-D$ kongruentna 1 ali 0 (mod 4) in nobeno liho praštevilo ne deli D s potenco več kot 1. Označimo z d tako kvadratov prosto celo število, da je $\mathbb{Q}(\tau) = \mathbb{Q}(\sqrt{-d})$. Povedano drugače, če je $d \equiv 3 \pmod 4$, potem velja $D = d$, če pa je $d \equiv 1, 2 \pmod 4$, potem velja $D = 4d$.

Za izračun Hilbertovega razrednega polinoma $H_D(x)$ definiranega v A.2.36 obstaja več načinov [13]. Mi bomo opisali klasični pristop, kjer je potrebno dovolj natančno izračunati vrednosti $j(\tau)$ za različne $\tau \in \mathcal{H}$. Pri tem si lahko pomagamo z naslednjimi formulami [17, poglavje III]:

$$h(\tau) = \frac{\Delta 2\tau}{\Delta(\tau)}, \quad j(\tau) = \frac{(256h(\tau)+1)^3}{h(\tau)},$$

kjer je

$$\Delta(\tau) = q\left(1 + \sum_{n\geq 1}(-1)^n(q^{n(3n-1)/2} + q^{n(3n+1)/2})\right)^{24} \quad \text{in} \quad q = e^{2\pi\sqrt{-1}\tau}.$$

Tako definirana funkcija $\Delta(\tau)$ je 24-ta potenca bolj znane **Dedekindova funkcija**, ki je definirana kot

$$\begin{aligned}\eta(\tau) &= \Delta(\tau)^{1/24} = q^{1/24}\prod_{n=1}^{\infty}(1-q^n) \\ &= e^{2\pi i\tau/24}\left(1 + \sum_{n\geq 1}(-1)^n(q^{n(3n-1)/2} + q^{n(3n+1)/2}).\right).\end{aligned}$$

Dedekindova funkcija zadošča naslednjima lastnostima:

$$\eta(\tau+1) = e^{2\pi i/24}\eta(\tau), \quad \eta(-1/\tau) = \sqrt{-i\tau}\eta(\tau).$$

Polinom $H_D(x)$ lahko izračunamo z aproksimacijo za $j(\tau)$ v produktu

$$H_D(x) = \prod_{\alpha}(x - j(\alpha)),$$

kjer je α oblike

$$\alpha = (-b + \sqrt{-D})/(2a)$$

in konstante a, b, c zadoščajo naslednjim pogojem: $b^2 - 4ac = -D$, $|b| \leq \sqrt{|D|/3}$, $a \leq c$, $\gcd(a, b, c) = 1$ in iz $|b| = a$ ali $a = c$ sledi $b \geq 0$. Povedano drugače, $ax^2 + bxy + cy^2$ je primitivna, reducirana pozitivno definitna binarna kvadratna forma z diskriminanto $-D$ [85].

Natančnost izračunov $j(\alpha)$ je pomembna, saj so zaradi ocene $\log|j(\alpha)| \approx \pi\sqrt{D}/a$ koeficienti polinoma $H_D(x)$ lahko zelo veliki.

Zgoraj napisano lahko posplošimo. V nadaljevanju si bomo podrobneje pogledali dodatne lastnosti eliptičnih krivulj nad končnimi obsegi in nato predstavili algoritem generiranja krivulj nad $\mathbb{F}_p$.

4.9.2 Eliptične krivulje s CM nad končnimi obsegi

Pri parjenjih nas bodo zanimale eliptične krivulje nad končnimi obsegi. V tem razdelku bomo opisali lastnosti kolobarja endomorfizmov teh krivulj, kajti kompleksno množenje v $\mathrm{End}(E)$ zagotovi, da ima krivulja E kompleksno množenje.

Trditev 4.9.10. *Eliptična krivulja nad končnim obsegom $\mathbb{F}_q$ ima vedno kompleksno množenje.*

Dokaz. Po [52] je Frobeniusov endomorfizem ϕ_q koren polinoma $X^2 - aX + q = 0$, kjer je $|a| \leq 2\sqrt{q}$. . Če je $|a| < 2\sqrt{q}$, potem ima ta polinom samo kompleksne ničle in $\phi_q \notin \mathbb{Z}$. Posledično $\mathbb{Z} \neq \mathbb{Z}[\phi_q] \subseteq \mathrm{End}(E)$. Če pa je $a = \pm 2\sqrt{q}$, je kolobar endomorfizmov še vedno večji od $\mathbb{Z}$, tako da ima E kompleksno množenje tudi v tem primeru. ■

Glavni izrek, ki opiše kolobar endomorfizmov eliptičnih krivulj E nad končnimo obsegi je naslednji. Dokaz izreka je na voljo tudi v [38].

Izrek 4.9.11. *[152, Izrek 10.6]. Naj bo E eliptična krivulja nad končnim obsegom karakteristike p.*

1. *Če je E navadna eliptična krivulja iz definicije 4.8.1, potem je* $\mathrm{End}(E)$ *red v imaginarnem kvadratnem obsegu.*

2. *Če je E supersingularna iz definicije 4.8.1, potem je* $\mathrm{End}(E)$ *maksimalen red v definitni algebri kvaternionov, ki je ramificiran v p in ∞ in je razcepen (ang. split) v drugih praštevilih.*

■

4.9.3 Generiranje krivulj s pomočjo CM

V tem razdelku bomo na kratko opisali osnove generiranja eliptičnih krivulj s pomočjo metode kompleksnega množenja. Na to temo obstaja veliko literature, na primer [17, 137, 152].

Metoda, ki jo bomo opisali, je namenjena generiranju krivulj nad velikimi praštevilskimi obsegi, za drugačne obsege glej [106, 152]. Metoda temelji na aritmetiki kompleksnih kvadratnih obsegov $K = \mathbb{Q}(\sqrt{-D})$, kjer je $-D$ diskriminanta, ki je osnovni vhodni podatek metode. Metoda je hitra, če je število razredov h_D obsega K majhno.

Želimo konstruirati krivuljo E nad obsegom $K = \mathbb{F}_p$ s kompleksnim množenjem, katerega diskriminanta reda $\mathrm{End}(E)$ je enaka $-D$. Po [137] j-invarianta take krivulje leži v $\mathbb{F}_p$ torej iščemo tako diskriminanto $-D$, za katero ima Hilbertov polinom $H_D(x)$ iz definicije A.2.36 koren v $\mathbb{F}_p$. Stolp obsegov $\mathbb{Q} \subset K \subset H$, kjer je H Hilbertov obseg razredov obsega K, se lokalno reducira ali na $\mathbb{Q}_p$, ali na njegovo kvadratno razširitev. Pri prvi možnosti se p v K razcepi, pri drugi pa p ostane praštevilo. Če p ostane praštevilo, potem krivulja po modulu p s kompleksnim množenjem v $\mathbb{Z}[\sqrt{-D}]$ ne obstaja.

Pri dani diskriminanti D torej iščemo praštevila p, ki se v K razcepijo v glavne praideale po definiciji A.2.24. Za tako praštevilo bo diofantska enačba

$$4p = x^2 + Dy^2 \tag{4.17}$$

rešljiva. Tako enačbo lahko rešimo s Cornacchiovim algoritmom, ki vrne verižne ulomke korena. Reševanje $4p = x^2 + Dy^2$ je ekvivalentno reševanju $p = u^2 + dv^2$, ki ga rešimo z naslednjim algoritmom.

Algoritem 4.9.1 uporabimo tako, da zaporedoma testiramo praštevila, dokler ne dobimo rešitve. Pričakovano število poskusov je $1/(2h_D)$ [17].

Iz rezultata, ki je trojka (x, y, p) izračunamo

$$m = p + 1 \pm x.$$

To je kandidat za možen red grupe eliptične krivulje nad $\mathbb{F}_p$, ki jo želimo konstruirati. Za m preverimo, če ustreza pogojem [17]: ima veliki praštevilski faktor, ni enak p in ne obstaja majhen k za katerega je $p^k \equiv 1 \pmod{m}$. Število točk na krivulji je po Hassejevem izreku 4.6.2 enako $m = p + 1 - t$, kjer je t Frobeniusova sled. Velja tudi $t = \alpha + \overline{\alpha}$, kjer je α element z normo enako p v obsegu K [17]. Rešitev enačbe $x^2 + Dy^2 = 4p$ pomeni, da je $\alpha = \pm(x + \sqrt{-D}y)/2$ element z normo enako p in sledjo enako $\pm x$. Redi $p + 1 \pm x$ bodo torej redi eliptične krivulje in njihovih kvadratnih ovojev [137].

Glavna ideja za konstrukcijo krivulje nad obsegom $\mathbb{F}_p$ z grupo reda m je v naslednji lemi.

Lema 4.9.12. *[17, Lema VIII.3]. Za obseg $\mathbb{F}_p$ veljajo naslednje trditve:*

1. *Vsak element v obsegu $\mathbb{F}_p$ je j-invarianta neke eliptične krivulje nad $\mathbb{F}_p$;*
2. *Če je $D > 4$ so vse krivulje z j-invarianto $j \neq 0, 1728$ nad obsegom $\mathbb{F}_p$ podane z enačbo*

$$Y^2 = X^3 + 3lc^2X + 2lc^3, \tag{4.18}$$

kjer je $l = j/(1728 - j)$ in $c \in \mathbb{F}_p$;

Algoritem 4.9.1 Cornacchiov algoritem

Vhodni podatki: celo število brez kvadratov d in praštevilo p.
Rezultat: Rešitev enačbe $p = u^2 + dv^2$, če obstaja.

1. Naj bo $p/2 < x_0 < p$ rešitev $x^2 \equiv -d \pmod{p}$;
2. $p \leftarrow q_0 x_0 + x_1$;
3. $k \leftarrow 0$;
4. **while** ${x_k}^2 < p \leq {x_{k-1}}^2$ **do**
   (a) $x_k \leftarrow q_{k+1} x_{k+1} + x_{k+2}$;
   (b) $k \leftarrow k + 1$;
5. **end while**
6. $u \leftarrow x_k$;
7. $v \leftarrow \sqrt{(p - {x_k}^2)/d}$;
8. **if** $v \in \mathbb{Z}$ **then**
   Vrni (u, v);
9. **else**
   Vrni "Ni rezultata";
10. **end if**

3. *Izberimo število j različno od 0 in 1728. Če imata E in E' enako j-invarianto, vendar nista izomorfni nad obsegom $\mathbb{F}_p$, potem je E' kvadratni ovoj E. Če velja še $\#E = p + 1 - t$, potem je $\#E' = p + 1 + t$;*

4. *Če je $j = 0$ ali $j = 1728$ moramo upoštevati ovoje višjih stopenj 4 ali 6.*

■

Naj bo $j \neq 0, 1728$, in E podana z enačbo

$$E: \ Y^2 = X^3 + aX + b.$$

Potem ima E' iz točke 3. zgornje leme enačbo

$$E': \ Y^2 = X^3 + ac^2X + bc^3,$$

kjer je c poljubno celo število, za katero enačba $x^2 \equiv c \pmod{p}$ nima rešitve v $\mathbb{F}_p$. To pomeni, da ko konstruiramo j-invarianto krivulje nad $\mathbb{F}_p$ reda m, dobimo dve kandidatki za enačbo krivulje. Katera je prava enostavno preverimo z naključnim izbiranjem točk. Problem konstrukcije krivulje smo tako reducirali na problem računanja možne j-invariante eliptične krivulje nad $\mathbb{F}_p$ z danim številom točk m in kompleksnim množenjem maksimalnega reda $\mathbb{Q}(\sqrt{-D})$. Take j-invariante morajo biti natanko koreni Hilbertovega polinoma $H_D(x)$ po modulu p. Tako je potrebno izračunati le Hilbertov polinom $H_D(x)$ in poiskati njegove korene. Obstajajo še izboljšave zgoraj opisanega algoritma, kjer uporabljamo Webrove polinome [82, 153].

Primer. Naj bo $D = 7$, iščemo praštevilo p za katero ima enačba

$$4p = x^2 + Dy^2$$

rešitev. Z izbiro naključnih praštevil in uporabo algoritma 4.9.1 dobimo rešitev

$$p = 781221660082682887337352611537.$$

Na podlagi te vrednosti za p iščemo eliptično krivuljo nad $\mathbb{F}_p$ z redom grupe

$$m = 781221660082681210712714541668,$$

kar je štirikratnik lihega praštevila. Število razredov reda obsega $K = \mathbb{Q}(\sqrt{-7})$ je enako ena. To pomeni, da ima Hilbertov polinom stopnjo ena in je enak

$$H_D(x) = x + 3375.$$

Pravimo, da ima $H_D(x)$ koren v $\mathbb{Z}/p\mathbb{Z} \simeq \mathbb{F}_p$. Potrebujemo torej eliptično krivuljo z j-invarianto

$$j_E = -3375 \equiv 781221660082682887337352608162 \pmod{p}.$$

Do izomorfizma natančno sta taki krivulji dve:

$$\begin{aligned} E: \ Y^2 = X^3 \ &+ \ 384410658135923325515205253294X \\ &+ \ 777088212145737475235038576554 \end{aligned}$$

in

$$\begin{aligned} E' :\ Y^2 = X^3 &+ 58633713708896852150756297732 9X \\ &+ 47061287768828409351193075021 3. \end{aligned}$$

Katera krivulja je prava, preverimo z naključnimi točkami. Kratek izračun pokaže, da je prava druga krivulja. •

Primer. Naj bo $D = 292$. Število razredov reda obsega $K = \mathbb{Q}(\sqrt{-D})$ je 4. Za praštevilo

$$p = 47106401771464858174371611525 3$$

je enačba $x^2 + Dy^2 = 4p$ rešljiva. Od tod sklepamo, da obstaja eliptična krivulje z grupo reda

$$m = 4710640177146476307254985828 02.$$

Hilbertov polinom $H_D(x)$ je enak

$$\begin{aligned} H_D(x) = x^4 &- 20628770986042830460800 0x^3 \\ &- 93693622511929038759497066112000000x^2 \\ &+ 45521551386379385369299683384000000000x \\ &- 38025946104251240477999064268800000000000000 \end{aligned}$$

in ima 4 korene $\pmod p$, ki so vrednosti štirih j-invariant eliptičnih krivulj nad $\mathbb{F}_p$ z grupami reda m. Ena izmed teh vrednosti je $j = 952981631055855428990768234 35$, iz katere lahko izračunamo naslednji dve eliptični krivulji:

$$\begin{aligned} E :\ Y^2 = X^3 &+ 46926843642824672578103513427 7X \\ &+ 15582428504728162327278471776 7 \end{aligned}$$

in

$$\begin{aligned} E :\ Y^2 = X^3 &+ 35461873957334781312338909332 4X \\ &+ 31425177859305436259087995457 4. \end{aligned}$$

Druga krivulja ima red enak m, medtem ko ima prva red enak $2(p + 1) - m$. •

Poglavje 5

PARJENJA NA ELIPTIČNIH KRIVULJAH

V drugem poglavju smo definirali bilinerano parjenje, ter navedli osnovne lastnosti in tipe. V tem poglavju si bomo ogledali parjenja na eliptičnih krivuljah. Pri tem bosta grupi G_1 in G_2 v definiciji 2.1 grupi oziroma podgrupi točk na eliptični krivulji. Za različne tipe parjenj bomo navedli možnosti implementacij na eliptičnih krivuljah. Nato bomo predstavili dva osnovna primera parjenj na eliptičnih krivuljah, Tate-Lichtenbaumovo parjenje in Weilovo parjenje. Navedena primera parjenj sta ključna v kriptografiji, saj je večina ostalih parjenj, kot na primer ate in eta, izpeljana iz njiju [65]. Na koncu bomo opisali Millerjev algoritem za računanje parjenj in distorzijske preslikave, ki jih izpeljemo iz parjenj.

5.1 Tipi parjenj

Spomnimo se iz poglavja 2, da imamo glede na oblike in lastnosti grup G_1 in G_2, štiri tipe parjenj [30, 56, 96]:

- **Tip 1**: $G_1 = G_2$;
- **Tip 2:** $G_1 \neq G_2$ in obstaja učinkovito izračunljiv netrivialni homomorfizem $\phi : G_2 \to G_1$;
- **Tip 3:** $G_1 \neq G_2$ in ne obstaja oziroma ni znanega učinkovito izračunljivega netrivialnega homomorfizma $\phi : G_2 \to G_1$ med grupama;
- **Tip 4:** $G_1 \subset G_2$, grupa G_1 je podgrupa grupe G_2.

Parjenja tipa 1 so implementirana na supersingularnih krivuljah, ki jih lahko razdelimo v dve skupini. V prvi skupini so supersingularne krivulje nad obsegi s karakteristiko 2 ($\mathbb{F}_{2^m}$) ali 3 ($\mathbb{F}_{3^m}$). Te imajo vključitveno stopnjo 4 oziroma 6. V drugi skupini pa so supersingularne krivulje nad praštevilskimi obsegi ($\mathbb{F}_p$), ki imajo vključitveno stopnjo enako 2. Parjenja tipa 2 so implementirana na navadnih krivuljah in homomorfizem $G_2 \to G_1$ je lahko kar sled definirana v 4.6.14. Parjenja tipa 3 so implementirana na navadnih krivuljah, kjer je G_2 ponavadi jedro sledi. Tip 3 je implementiran nad praštevilskimi

obsegi $\mathbb{F}_p$. Parjenja tipa 4 so implementirana na navadnih krivuljah, pri čemer je grupa G_2 kar cela grupa q-torzijskih točk $E[q]$.

5.2 Weilovo parjenje

Weilovo parjenje na n-torzijskih točkah eliptične krivulje je pomembno orodje pri študiju in uporabi eliptičnih krivulj. Z njim lahko dokažemo Hassejev izrek 4.6.2, uporabljeno je v napadu na diskretni logaritem na eliptičnih krivuljah, pojavlja pa se tudi v mnogo protokolih in shemah, ki temeljijo na parjenjih.

Naj bo E eliptična krivulja nad obsegom K in naj bo n naravno število, ki ni deljivo s karakteristiko obsega K. Po izreku 4.5.4 je grupa n-torzijskih točk enaka $E[n] \simeq \mathbb{Z}_n \oplus \mathbb{Z}_n$. Naj bo $\mu_n = \{x \in \overline{K},\ x^n = 1\}$ grupa n-tih korenov enote v $\overline{K}$. Povzemimo lastnosti korenov enot iz dodatka A.2.6. Ker n ne deli karakteristike K, enačba $x^n = 1$ nima večkratnih ničel [93] in ima zato n korenov v $\overline{K}$. Grupa μ_n je ciklična reda n in vsak njen generator ζ imenujemo primitivni koren enote; to je ekvivalentno temu, da je $\zeta^k = 1$ natanko tedaj, ko n deli k. Naj bo $E[n] \subseteq E(K)$ in kot bomo dokazali kasneje v trditvi 5.2.2, velja $\mu_n \subset K$.

Želeli bi konstruirati parjenje

$$e_n : E[n] \times E[n] \to \mu_n.$$

Izberimo točko $T \in E[n]$. Po posledici 4.2.8 obstaja funkcija f, za katero velja

$$\operatorname{div}(f) = n(T) - n(\mathcal{O}). \tag{5.1}$$

Naj bo $T' \in E[n^2]$ taka točka, da velja $nT' = T$. S pomočjo posledice 4.2.8 bomo pokazali, da obstaja taka funkcija g, za katero velja

$$\operatorname{div}(g) = \sum_{R \in E[n]} \left((T' + R) - (R)\right). \tag{5.2}$$

Preveriti je potrebno, da je vsota točk v zgornjem delitelju enaka $\mathcal{O}$. To sledi iz dejstva, da $E[n]$ vsebuje n^2 točk. Točke R se v $\sum(T'+R)-\sum(R)$ odštejejo in vsota je $n^2T' = nT = \mathcal{O}$. Funkcija g je neodvisna od izbire točke T', saj se vsaki dve izbiri T' med seboj razlikujeta za element $R \in E[n]$. Tako lahko napišemo tudi

$$\operatorname{div}(g) = \sum_{nT''=T} (T'') - \sum_{nR=\mathcal{O}} (R).$$

Naj $f \circ [n] :\ E \to \overline{K}$ označuje funkcijo, ki je kompozitum množenja z n in funkcije f. Opazimo, da so točke oblike $T' + R$, kjer je $R \in E[n]$, natanko tiste točke, za katere velja $n(T' + R) = T$. Iz (5.1) sledi

$$\operatorname{div}(f \circ [n]) = n\left(\sum_{R \in E[n]} (T' + R)\right) - n\left(\sum_{R \in E[n]} (R)\right) = \operatorname{div}(g^n).$$

Posledično je $f \circ [n]$ enaka g^n pomnoženi s konstantnim faktorjem.

Izberimo poljubni $S \in E[n]$ in $P \in E(\overline{K})$, za kateri sta $g(P+S)$ in $g(P)$ definirani in neničelni. Potem velja

$$g(P+S)^n = f(n[P+S]) = f(nP) = g(P)^n.$$

Posledično je $g(P+S)/g(P) \in \mu_n$. Pri tem je vrednost $g(P+S)/g(P)$ neodvisna od izbire P [152, poglavje 11].

Zdaj lahko definiramo **Weilovo parjenje** kot:

$$e_n(S,T) = \frac{g(P+S)}{g(P)}. \tag{5.3}$$

Definicija je neodvisna od izbire g v (5.2), saj je g določena z deliteljem do skalarnega večkratnika natančno. Prav tako je e_n neodvisna od izbire pomožne točke P. Glavne lastnosti tako definiranega parjenja so zajete v naslednjem izreku.

Izrek 5.2.1. *Naj bo E eliptična krivulja definirana nad obsegom K in naj bo n tako naravno število, ki ni deljivo s karakteristiko K. Potem je*

$$e_n : E[n] \times E[n] \to \mu_n,$$

definirano v (5.3) *parjenje z naslednjimi lastnostmi:*

1. *e_n je bilinearno v obeh spremenljivkah, kar pomeni:*

$$e_n(S_1+S_2,T) = e_n(S_1,T)e_n(S_2,T),$$

$$e_n(S,T_1+T_2) = e_n(S,T_1)e_n(S,T_2),$$

   za vsak $S, S_1, S_2, T, T_1, T_2 \in E[n]$;

2. *e_n je neizrojeno v obeh spremenljivkah, kar pomeni:*

$$\begin{array}{llll} iz & e_n(S,T)=1 & za\ vsak & T \in E[n] \quad sledi \quad S=\mathcal{O}, \\ iz & e_n(S,T)=1 & za\ vsak & S \in E[n] \quad sledi \quad T=\mathcal{O}; \end{array}$$

3. *$e_n(T,T) = 1$ za vsak $T \in E[n]$;*

4. *$e_n(T,S) = e_n(S,T)^{-1}$ za vsak $S,T \in E[n]$;*

5. *$e_n(\sigma(S),\sigma(T)) = \sigma(e_n(S,T))$ za vsak tak avtomorfizem σ obsega $\overline{K}$, ki na koeficientih krivulje E deluje kot identiteta;*

6. *$e_n(\alpha(S),\alpha(T)) = e_n(S,T)^{\deg(\alpha)}$ za vsak separabilen avtomorfizem α krivulje E. V primeru ko koeficienti krivulje E ležijo v obsegu $\mathbb{F}_q$, trditev velja tudi za Frobeniusov endomorfizem $\alpha = \phi_q$.*

Dokaz.

1. Ker je e_n neodvisen od izbire točke P, lahko uporabimo (5.3) s P in $P + S_1$ da dobimo
$$\begin{aligned} e_n(S_1, T)e_n(S_2, T) &= \frac{g(P + S_1)}{g(P)} \frac{g(P + S_1 + S_2)}{g(P + S_1)} \\ &= \frac{g(P + S_1 + S_2)}{g(P)} \\ &= e_n(S_1 + S_2, T). \end{aligned}$$
To dokaže linearnost v prvi spremenljivki. Naj bodo $T_1, T_2, T_3 \in E[n]$, kjer je $T_1 + T_2 = T_3$. Točke T_i določijo funkcije f_i, g_i za $1 \leq i \leq 3$ v definiciji Weilovega parjenja za $e_n(S, T_i)$. Po posledici 4.2.8 obstaja taka funkcija h, da je
$$\operatorname{div}(h) = (T_3) - (T_1) - (T_2) - (\mathcal{O}).$$
Iz enačbe (5.1) sledi
$$\operatorname{div}\left(\frac{f_3}{f_1 f_2}\right) = n \cdot \operatorname{div}(h) = \operatorname{div}(h^n).$$
Posledično obstaja neničelni $c \in \overline{K}$, tako da je
$$f_3 = c f_1 f_2 h^n,$$
odkoder sklepamo
$$g_3 = c^{1/n}(g_1)(g_2)(h \circ [n]).$$
Po definiciji parjenja e_n dobimo
$$\begin{aligned} e_n(S, T_1 + T_2) &= \frac{g_3(P + S)}{g_3(P)} \\ &= \frac{g_1(P + S)}{g_1(P)} \frac{g_2(P + S)}{g_2(P)} \frac{h(n[P + S])}{h(nP)} \\ &= e_n(S, T_1)e_n(S, T_2). \end{aligned}$$
Res, ker je $nS = \mathcal{O}$, je $h(n[P + S]) = h(nP)$. To dokaže linearnost v drugi spremenljivki.

2. Naj bo $T \in E[n]$ z lastnostjo $e_n(S, T) = 1$ za vsak $S \in E[n]$. Posledično velja $g(P + S) = g(P)$ za vsak $P, S \in E[n]$. Po trditvi 4.5.5 obstaja taka funkcija h, da $g = h \circ [n]$. Velja
$$(h \circ [n])^n = g^n = f \circ [n].$$
Ker je množenje z n po trditvi 4.3.2 in izreku 3.2.7 surjektivna preslikava na $E(\overline{K})$, je $h^n = f$. Torej je
$$n \cdot \operatorname{div}(h) = \operatorname{div}(f) = n(T) - n(\mathcal{O})$$
in $\operatorname{div}(H) = (T) - (\mathcal{O})$. Po posledici 4.2.8 je $T = \mathcal{O}$. Tako smo dokazali prvi del. Neizrojenost v S sledi iz točke 4. izreka in neizrojenosti v točki T.

3. Naj τ_{jT} predstavlja seštevanje z jT, tako da $f \circ \tau_{jT}$ deluje po predpisu

$$P \mapsto f(P + jT).$$

Delitelj $f \circ \tau_{jT}$ je enak $n(T - jT) - n(-jT)$. Velja

$$\operatorname{div}\left(\prod_{j=0}^{n-1} f \circ \tau_{jT}\right) = \sum_{j=0}^{n-1} (n([1-j]T) - n(-jT)) = 0.$$

To pomeni, da je $\prod_{j=0}^{n-1} f \circ \tau_{jT}$ konstantna. Ker je $nT' = T$ sklepamo, da je konstantna tudi

$$\begin{aligned}\left(\prod_{j=0}^{n-1} g \circ \tau_{jT'}\right)^n &= \prod_{j=0}^{n-1} f \circ [n] \circ \tau_{jT'} \\ &= \prod_{j=0}^{n-1} f \circ \tau_{jT} \circ [n].\end{aligned}$$

Posledično je $\prod_{j=0}^{n-1} g \circ \tau_{jT'}$ tudi konstantna in zato zavzame enaki vrednosti pri P in $P + T'$. Torej velja

$$\prod_{j=0}^{n-1} g(P + T' + jT') = \prod_{j=0}^{n-1} g(P + jT').$$

Po krajšanju skupnih faktorjev dobimo

$$g(P + nT') = g(P).$$

Ker je $nT' = T$, smo dokazali

$$e_n(T, T) = \frac{g(P+T)}{g(P)} = 1.$$

4. Po točki 1. in 3. izreka velja

$$\begin{aligned}1 &= e_n(S+T, S+T) \\ &= e_n(S,S)e_n(S,T)e_n(T,S)e_n(T,T) \\ &= e_n(S,T)e_n(T,S).\end{aligned}$$

Posledično je $e_n(T,S) = e_n(S,T)^{-1}$.

5. Naj bo σ tak avtomorfizem obsega $\overline{K}$, ki je identiteta na koeficientih krivulje E. Z f^σ in g^σ označimo funkciji dobljeni z delovanjem σ na koeficientih racionalnih funkcij, ki definirata f in g v konstrukciji parjenja e_n. Izračunajmo

$$\operatorname{div}(f^\sigma) = n(\sigma T) - n(\mathcal{O})$$

in podobno naredimo za g^σ. Posledično velja

$$\sigma(e_n(S,T)) = \sigma\left(\frac{g(P+S)}{g(P)}\right) = \frac{g^\sigma(\sigma P + \sigma S)}{g^\sigma(\sigma P)} = e_n(\sigma S, \sigma T).$$

6. Naj bo α separabilen avtomorfizem krivulje E in $\{Q_1, \ldots, Q_k\} = \ker(\alpha)$. Po trditvi 3.2.17 je $\deg(\alpha) = k$. Naj za racionalni funkciji f_T in $f_{\alpha(T)}$ velja

$$\mathrm{div}(f_T) = n(T) - n(\mathcal{O}), \quad \mathrm{div}(f_{\alpha(T)}) = n(\alpha(T)) - n(\mathcal{O}).$$

Definirajmo racionalni funkciji g_T^n in $g_{\alpha(T)}^n$ kot kompozituma

$$g_T^n = f_T \circ [n], \quad g_{\alpha(T)}^n = f_{\alpha(T)} \circ [n].$$

Kot v točki 3. naj τ_Q označuje seštevanje s Q. Potem velja

$$\mathrm{div}(f_T \circ \tau_{-Q_i}) = n(T + Q_i) - n(Q_i)$$

in posledično je

$$\begin{aligned} \mathrm{div}(f_{\alpha(T)} \circ \alpha) &= \sum_{\alpha(T'')=\alpha(T)} (T'') - n \sum_{\alpha(Q)=\mathcal{O}} (Q) \\ &= n \sum_i ((T + Q_i) - (Q_i)) \\ &= \mathrm{div}(\prod_i (f_T \circ \tau_{-Q_i})). \end{aligned}$$

Za vsak i izberemo tako točko Q_i', da je $nQ_i' = Q_i$. Iz enakosti $g_T(P - Q_i') = f_T(nP - Q_i)$ sklepamo

$$\begin{aligned} \mathrm{div}\left(\prod_i (g_T \circ \tau_{-Q_i'})^n\right) &= \mathrm{div}\left(\prod_i f_T \circ \tau_{-Q_i} \circ [n]\right) \\ &= \mathrm{div}(f_{\alpha(T)} \circ \alpha \circ [n]) \\ &= \mathrm{div}(f_{\alpha(T)} \circ [n] \circ \alpha) \\ &= \mathrm{div}(g_{\alpha(T)} \circ \alpha)^n. \end{aligned}$$

Poleg tega imata funkciji $\prod_i g_T \circ \tau_{-Q_i'}$ in $g_{\alpha(T)} \circ \alpha$ enak delitelj, torej je njun kvocient konstanten.

Iz definicije (5.3) parjenja e_n sledi

$$\begin{aligned} e_n(\alpha(S), \alpha(T)) &= \frac{g_{\alpha(T)}(\alpha(P + S))}{g_{\alpha(T)}(\alpha(P))} \\ &= \prod_i \frac{g_T(P + S - Q_i')}{g_T(P - Q_i')} \\ &= \prod_i e_n(S, T) \\ &= e_n(S, T)^k = e_n(S, T)^{\deg(\alpha)}. \end{aligned}$$

Če je $\alpha = \phi_q$ Frobeniusov endomorfizem, potem iz točke 5. sklepamo,

$$e_n(\phi_q(S), \phi_q(T)) = \phi_q(e_n(S, T)) = e_n(S, T)^q,$$

saj je ϕ_q q-ta potenca elementov v $\overline{\mathbb{F}}_q$. Iz trditve 3.2.16 sledi, da je $q = \deg(\phi_q)$, s čimer je točka 6. izreka dokazana.

■

Posledica 5.2.2. *Ob predpostavki izreka 5.2.1 obstajata taki točki $S, T \in E[n]$, za kateri je $e_n(S,T)$ primitivni n-ti koren enote. Če je $E[n] \subset E(K)$, potem je $\mu_n \subset K^*$.*

Dokaz. Za poljubni točki $S, T \in E[n]$ je $e_n(S,T)$ element podgrupe μ_d grupe μ_n. Za vsak $S, T \in E[n]$ torej velja

$$1 = e_n(S,T)^d = e_n(dS,T).$$

Ker je e_n neizrojeno, je $dS = \mathcal{O}$ in ker je točka S poljubna, sledi $d = n$. Če je $E[n] \subset E(K)$, potem iz točke 5. izreka 5.2.1 sklepamo, da je $e_n(S,T) \in K^*$ za vsak $S, T \in E[n]$. Torej je tudi $\mu_n \subset K^*$. ■

Za eliptični krivulji E_1 in E_2 in izogenijo $\phi : E_1 \to E_2$ po definiciji 4.3.10, obstaja dualna izogenija $\hat{\phi} : E_2 \to E_1$. Naslednja trditev pokaže, kako sta si ϕ in $\hat{\phi}$ dualni glede na parjenje.

Trditev 5.2.3. *Naj bosta $S \in E_1[n]$ in $T \in E_2[n]$ in naj bo $\phi : E_1 \to E_2$ izogenija. Potem velja*

$$e_n(S, \hat{\phi}(T)) = e_n(\phi(S), T).$$

Dokaz. Naj bo f racionalna funkcija, za katero velja $\mathrm{div}(f) = n(T) - n(\mathcal{O})$, in g^n kompozitum funkcij definiran s pravilom $g^n = f \circ [n]$. Potem je

$$e_n(\phi(S), T) = \frac{g(P + \phi(S))}{g(P)}.$$

Izberimo tako funkcijo $h \in \overline{K}(E_1)$, da za ϕ^* v predpisu (3.9) velja

$$\phi^*((T)) - \phi^*((\mathcal{O})) = (\hat{\phi}(T)) - (\mathcal{O}) + \mathrm{div}(h).$$

Taka funkcija h obstaja, saj je po točki 2. izreka 4.3.9 $\hat{\phi}(T)$ natanko vsota točk delitelja na levi strani te enačbe. Potem je

$$\mathrm{div}\left(\frac{f \circ \phi}{h^n}\right) = \phi^* \mathrm{div}(f) - n\mathrm{div}(h) = n(\hat{\phi}(T)) - n(\mathcal{O})$$

in

$$\begin{aligned}\left(\frac{g \circ \phi}{h \circ [n]}\right)^n &= \frac{f \circ [n] \circ \phi}{(h \circ [n])^n} \\ &= \left(\frac{f \circ \phi}{h^n}\right) \circ [n].\end{aligned}$$

Iz definicije parjenja e_n sledi

$$\begin{aligned}e_n(S, \hat{\phi}(T)) &= \frac{(g \circ \phi / h \circ [n])(P + S)}{(g \circ \phi / h \circ [n])(P)} \\ &= \frac{g(\phi(P) + \phi(S))}{g(\phi(P))} \frac{h(nP)}{h(nP + nS)} \\ &= e_n(\phi(S), T).\end{aligned}$$

■

Pri računanju zgoraj definiranega Weilovega parjenja lahko uporabimo princip, ki smo ga videli na primeru v razdelku 4.2 o grupi na eliptičnih krivuljah. Ker definicija vsebuje funkcijo g, katere delitelj vsebuje prispevke vseh n^2 točk v $E[n]$, je tako računanje v primeru velikih n zamudno. Zato v praksi uporabljamo alternativno definicijo Weilovega parjenja, ki jo bomo predstavili v nadaljevanju.

Izrek 5.2.4. *Naj bosta $S, T \in E[n]$. Izberimo disjunktna delitelja $D_S = \sum_P s_P(P)$ in $D_T = \sum_P t_P(P)$ stopnje 0, z lastnostjo $\sum s_P P = S$ in $\sum t_P P = T$. Naj bosta f_T in f_S funkciji za kateri je* $\mathrm{div}(f_S) = nD_S$ *in* $\mathrm{div}(f_T) = nD_T$. *Potem je Weilovo parjenje podano z*

$$e_n(S,T) = \frac{f_T(D_S)}{f_S(D_T)},$$

kjer je po definiciji $f(\sum a_i(P_i)) = \prod_i f(P_i)^{a_i}$.

Naravna izbira deliteljev v izreku 5.2.4 je

$$D_S = (S) - (\mathcal{O}), \quad D_T = (T+R) - (R),$$

za neko poljubno točko $R \in E(\overline{K})$. Preden dokažemo izrek 5.2.4, pa potrebujemo še nekaj vmesnih rezultatov, katerih dokazi so na voljo v [152, poglavje 11]. V nadaljevanju tega razdelka bomo uporabljali naslednje oznake:
Naj bosta $V, W \in E[n^2]$ in f_{nV} racionalna funkcija za katero velja

$$\mathrm{div}(f_{nV}) = n(nV) - n(\mathcal{O}).$$

Funkcija g_{nV} je definirana z $g_{nV}^n = f_{nV} \circ [n]$ kot v prvi definiciji Weilovega parjenja (5.3). Naj bosta

$$c(nV, nW) = \frac{f_{nV+nW}(X)}{f_{nV}(X) f_{nW}(X - nV)}, \tag{5.4}$$

$$d(V, W) = \frac{g_{nV+nW}(X)}{g_{nV}(X) g_{nW}(X - V)}, \tag{5.5}$$

kjer sta desni strani obeh enačb funkciji spremenljivke $X \in E(K)$.

Naslednja lema razloži, zakaj sta (5.4) in (5.5) neodvisni od spremenljivke X.

Lema 5.2.5. *$c(nV, vW)$ in $d(V, W)$ sta konstanti in*

$$d(V,W)^n = c(nV, nW).$$

■

Naslednje leme bodo povezale Weilovo parjenje z zgornjima c in d.

Lema 5.2.6. *Za točke $U, V, W \in E[n^2]$ veljajo enakosti:*

$$d(V, W + nU) = d(V,W) \quad in \quad d(V + nU, W) = d(V,W) e_n(nU, nW); \tag{5.6}$$

$$\frac{d(U,V)}{d(V,U)} = \frac{d(V,W) d(U+W,V)}{d(V,U+W) d(W,V)}. \tag{5.7}$$

■

Lema 5.2.7. *Naj bosta $S, T \in E[n]$. Potem je*

$$e_n(S,T) = \frac{c(S,T)}{c(T,S)}.$$

Dokaz. Izberimo $U, V \in E[n^2]$ za kateri velja $nU = S$, $nV = T$. Leva stran enakosti (5.7) ni odvisna od W, zato v desni strani vzamemo $W = jU$ za $0 \leq j < n$. Tako dobimo

$$\frac{c(nU,nV)}{c(nV,nU)} = \left(\frac{d(U,V)}{d(V,U)}\right)^n = \prod_{j=0}^{n-1} \frac{d(V,jU)d(U+jU,V)}{d(V,U+jU)d(jU,V)}.$$

Po krajšanju faktorjev dobimo

$$\frac{c(S,T)}{c(T,S)} = \frac{d(V,\mathcal{O})d(nU,V)}{d(V,nU)d(\mathcal{O},V)}.$$

Uporabimo enakost (5.6), kjer v prvi enačbi izberemo $W = \mathcal{O}$, da dobimo $d(V,nU) = d(V,\mathcal{O})$. V drugi enačbi (5.6) pa vzamemo $V = \mathcal{O}$ in $W = V$, da dobimo $d(nU,V) = d(\mathcal{O},V)e_n(nU,nV)$. ■

Zdaj imamo vse potrebno za dokaz izreka 5.2.4.

Dokaz. (Izrek 5.2.4.) Po definiciji c velja

$$e_n(S,T) = \frac{c(S,T)}{c(T,S)} = \frac{f_T(X)f_S(X-T)}{f_S(X)f_T(X-S)}, \tag{5.8}$$

kar je neodvisno od izbire X. Naj bosta

$$D'_S = (S) - (\mathcal{O}), \quad D'_T = (X_0) - (X_0 - T),$$

kjer X_0 izberemo tako, da imata D'_S in D'_T disjunktni podpori. Označimo $F'_S(X) = f_S(X)$ in $F'_T(X) = 1/f_T(X_0 - X)$. Potem velja

$$\operatorname{div}(F'_S) = n(S) - n(\mathcal{O}) = nD'_S$$

in

$$\operatorname{div}(F'_T) = n(X_0) - n(X_0 - T) = nD'_T.$$

To vstavimo v enakost v (5.8) in dobimo

$$e_n(S,T) = \frac{F'_T(D'_S)}{F'_S(D'_T)}.$$

S tem je izrek za zgoraj izbrana D'_S in D'_T dokazan. Potrebno je dokazati še neodvisnost od izbire.

Naj bosta zdaj $D_S = \sum_P s_P(P)$ in $D_T = \sum_P t_P(P)$ taka delitelja stopnje 0, za katera je $\sum s_P P = S$ in $\sum t_P P = T$. Potem je $D_S = \operatorname{div}(h_1) + D'_S$ in $D_T = \operatorname{div}(h_2) + D'_T$ za neki racionalni funkciji h_1 in h_2. Naj bosta $F_S = h_1^n F'_S$ in $F_T = h_2^n F'_T$. Potem je $nD_S = \operatorname{div}(F_S)$ in $nD_T = \operatorname{div}(F_T)$.

Če velja $(\mathrm{Supp}D_S \cup \mathrm{Supp}D'_S) \cap (\mathrm{Supp}D_T \cup \mathrm{Supp}D'_T) = \emptyset$, potem je

$$\frac{F_T(D_S)}{F_S(D_T)} = \frac{h_2(D_S)^n F'_T(D_S)}{h_1(D_T)^n F'_S(D_T)} = \frac{h_2(\mathrm{div}(h_1))^n h_2(D'_S)^n F'_T(\mathrm{div}(h_1)) F'_T(D'_S)}{h_1(\mathrm{div}(h_2))^n h_1(D'_T)^n F'_S(\mathrm{div}(h_2)) F'_S(D'_T)}.$$

Po Weilovem izreku o recipročnosti 3.3.13 velja $h_2(\mathrm{div}(h_1)) = h_1(\mathrm{div}(h_2))$ in

$$h_2(D'_S)^n = h_2(nD'_S) = h_2(\mathrm{div}(F'_S)) = F'_S(\mathrm{div}(h_2)),$$
$$h_1(D'_T)^n = h_1(nD'_T) = h_1(\mathrm{div}(F'_T)) = F'_T(\mathrm{div}(h_1)).$$

Tako dobimo

$$\frac{F_T(D_S)}{F_S(D_T)} = \frac{F'_T(D'_S)}{F'_S(D'_T)} = e_n(S,T).$$

Če pa $(\mathrm{Supp}D_S \cup \mathrm{Supp}D'_S) \cap (\mathrm{Supp}D_T \cup \mathrm{Supp}D'_T) \neq \emptyset$, dokažemo rezultat v dveh korakih. Naj bosta

$$D''_S = (X_1 + S) - (X_1), \quad D''_T = (Y_1 + T) - (Y_1),$$

delitelja, kjer sta X_1 in Y_1 izbrani tako, da velja

$$\begin{array}{rcl} (\mathrm{Supp}D'_S \cup \mathrm{Supp}D''_S) \cap (\mathrm{Supp}D'_T \cup \mathrm{Supp}D''_T) & = & \emptyset \text{ in} \\ (\mathrm{Supp}D''_S \cup \mathrm{Supp}D_S) \cap (\mathrm{Supp}D''_T \cup \mathrm{Supp}D_T) & = & \emptyset. \end{array}$$

Po že dokazanem sledi

$$\frac{F_T(D_S)}{F_S(D_T)} = \frac{F''_T(D''_S)}{F''_S(D''_T)} = \frac{F'_T(D'_S)}{F'_S(D'_T)} = e_n(S,T).$$

■

5.3 Tate-Lichtenbaumovo parjenje

V tem razdelku si bomo ogledali drugi pomemben primer parjenja. Podobno kot za Weilovo parjenje tudi za to obstajata dve ekvivalentni definiciji.

Izrek 5.3.1. *Naj bo E eliptična krivulja nad obsegom $\mathbb{F}_q$ in naj $n \in \mathbb{N}$ deli $q-1$. Označimo $\mu_n = \{x \in \mathbb{F}_q : \ x^n = 1\}$. Obstajata neizrojeni bilinearni parjenji*

$$\langle ., . \rangle_n : \ E(\mathbb{F}_q)[n] \times E(\mathbb{F}_q)/nE(\mathbb{F}_q) \to \mathbb{F}_q^*/(\mathbb{F}_q^*)^n \tag{5.9}$$

in

$$\tau_n : \ E(\mathbb{F}_q)[n] \times E(\mathbb{F}_q)/nE(\mathbb{F}_q) \to \mu_n, \tag{5.10}$$

kjer so $E(\mathbb{F}_q)[n]$ točke na $E(\mathbb{F}_q)$, katerih red deli n.

Prvemu parjenju pravimo **Tate-Lichtenbaumovo parjenje**, drugemu **modificirano Tate-Lichtenbaumovo parjenje**. Slednje je bolj primerno za računanje, saj je rezultat ekspliciten element v μ_n, medtem ko je slika prvega odsek v $\mathbb{F}_q^*$ po modulu n-te potence. Za tako definirana parjenja, bi praviloma morali pisati $\langle P, Q + nE(\mathbb{F}_q)\rangle_n$, podobno tudi za τ_n, saj so elementi v $E(\mathbb{F}_q)/nE(\mathbb{F}_q)$ oblike $Q + nE(\mathbb{F}_q)$. Vendar bomo v nadaljevanju ta zapis poenostavili v $\langle P, Q\rangle_n$ in $\tau(P, Q)$.

Za dokaz izreka 5.3.1 potrebujemo nekaj vmesnih rezultatov.

Lema 5.3.2. *Naj bo E eliptična krivulja nad obsegom $\mathbb{F}_q$. Izberimo delitelj D_1, ki se ohrani s q-tim Frobeniusovim endomorfizmom $\phi(D_1) = D_1$. Naj bo $S \subset E(\overline{\mathbb{F}}_q)$ dana končna množica točk. Potem obstaja tak delitelj D, ki se od D_1 razlikuje za glavni delitelj, velja $\phi(D) = D$, in D v svoji podpori ne vsebuje nobene točke iz S.*

Dokaz. Naj bo $D_1 = \sum_{j=1}^{d} cj(P_j)$. Ker točke P_j ležijo v neki končni množici grupe $E(\mathbb{F}_{q^k})$, obstaja $M \in \mathbb{N}$, da je $MP_j = \mathcal{O}$ za vsak j. Izberimo $m \equiv 1 \pmod{M}$ in $T \in E(\mathbb{F}_{q^k})$. Potem je $\phi^m(T) = T$, torej ϕ permutira množico $\{T, \phi(T), \ldots, \phi^{m-1}(T)\}$. Definirajmo

$$D = \sum_{i=0}^{m-1} \sum_{j=1}^{d} c_j \left((P_j + \phi^i(T)) - (\phi^i(T)) \right).$$

Ker je $\phi(D_1) = D_1$, je $\phi(P_j) = P_{j'}$ za vsak j in nek j', v posebnem je $c_j = c_{j'}$ za nek j'. Frobeniusov endomorfizem ϕ permutira točke, torej je $\phi(D) = D$. Spomnimo se definicije sum v (4.10). Ker je $m \equiv 1 \pmod{M}$, velja

$$\operatorname{sum}\left(\sum_{i=0}^{m-1} \left((P_j + \phi^i(T)) - (\phi^i(T)) \right) \right) = mP_j = P_j.$$

Posledično je $\operatorname{sum}(D_1 - D) = 0$ in $\deg(D_1 - D) = 0$, kar pomeni, da je $D_1 - D$ glavni delitelj.

Če D vsebuje točko iz množice S, potem velja ali $\phi^i(T) \in S$ ali $P_j + \phi^i(T) \in S$ za neka i in j. To pomeni, da je T vsebovan v množici dobljeni s translacijo množice $\phi^{-i}(S)$ za ali $\mathcal{O}$ ali za eno izmed točk $\phi^{-i}(P_j)$. Naj bo $s = \#S$. Potem je kvečjemu $m(d+1)s$ točk v uniji teh transliranih množic. Po Hassejevem izreku grupa $E(\mathbb{F}_{q^m})$ vsebuje vsaj $q^m + 1 - 2q^{m/2}$ točk. Ker je

$$\lim_{m \to \infty} \#E(\mathbb{F}_{q^m}) - m(d+1)s = \infty,$$

lahko s smiselno izbiro m najdemo tak T, da ni v uniji teh množic. Tako dobimo delitelj, ki v svoji podpori ne vsebuje točk iz S. ■

Lema 5.3.3. *Naj bo D' glavni delitelj za katerega je $\phi(D') = D'$ za q-ti Frobeniusov endomorfizem. Potem obstaja taka racionalna funkcija f, da je $\operatorname{div}(f) = D'$ in $f^\phi = f$, kjer je f^ϕ delovanje ϕ na koeficientih f. Funkcija f je torej definirana nad $\mathbb{F}_q$.*

Dokaz. Naj bo f_1 racionalna funkcija definirana nad $\overline{\mathbb{F}}_q$, za katero velja $\operatorname{div}(f_1) = D'$. Potem je

$$\operatorname{div}(f_1^\phi) = \phi(D') = D' = \operatorname{div}(f_1),$$

torej je $f_1^\phi / f_1 = c \in \overline{\mathbb{F}}_q^*$ konstanta. Izberimo tak $d \in \overline{\mathbb{F}}_q^*$, da je $c = d^{q-1} = \phi(d)/d$. Potem je

$$\phi(d)/d = c = f_1^\phi / f_1$$

in

$$((1/d)f_1)^\phi = (1/\phi(d))f_1^\phi = (1/d)f_1.$$

Ker je d konstanta, ima funkcija $f = (1/d)f_1$ enak delitelj kot f_1. ■

Zdaj imamo vse potrebno za dokaz izreka 5.3.1.

Dokaz. (Izrek 5.3.1.) Glavna ideja dokaza je naslednja. Naj bo $P \in E(\mathbb{F}_q)[n]$ in f taka, da bo $\mathrm{div}(f) = n((P) - (\mathcal{O}))$. Za $Q \in E(\mathbb{F}_q)$ izberimo delitelj $D_Q = \sum a_i(Q_i)$, ki je ekvivalenten delitelju $(Q) - (\mathcal{O})$ po modulu glavnih deliteljev in da v podpori ne vsebuje točk P ali $\mathcal{O}$. Potem velja

$$\langle P, Q\rangle_n = f(D_Q) = \prod_i f(Q_i)^{a_i}.$$

Vendar pa moramo biti pri zgornji izbiri deliteljev in funkcij previdni. Naj bo $P \in E(\mathbb{F}_q)[n]$ in D_P delitelj stopnje 0, za katerega je $\mathrm{sum}(D_P) = P$. To pomeni, da ima delitelj $D_P - (P) + (\mathcal{O})$ stopnjo 0 in sum enak $\mathcal{O}$, torej je delitelj neke racionalne funkcije. Drugače povedano, D_P je ekvivalenten $(P) - (\mathcal{O})$ po modulu glavnih deliteljev. Poleg tega predpostavimo, da je $\phi(D_P) = D_P$, kar pomeni da q-ti Frobeniusov endomorfizem ϕ permutira točke v D_P na tak način, da delitelj ostane nespremenjen. Po lemi 5.3.2 je možnosti za izbiro takih parametrov veliko.

Privzemimo, da smo izbrali ustrezen D_P. Potem obstaja funkcija f, da je

$$\mathrm{div}(f) = nD_P.$$

Vendar pa poleg tega želimo še $\phi\left((f(X)\right) = f^{\phi}(\phi(X))$ za vsak $X \in E(\overline{\mathbb{F}}_q)$. Obstoj take funkcije z lastnostjo $f^{\phi} = f$ zagotavlja lema 5.3.3. Izberimo $D_Q = \sum_i a_i(Q_i)$ delitelj stopnje 0, za katerega je $\mathrm{sum}(D_Q) = Q$, podpori D_P in D_Q nimata nobene skupne točke in velja $\phi(D_Q) = D_Q$. Definirajmo

$$\langle P, Q\rangle_n = f(D_Q) \pmod{(\mathbb{F}_q^*)^n},$$

kjer za vsako funkcijo f, katere delitelj nima skupnih točk z D_Q definiramo

$$f(D_Q) = \prod_i f(Q_i)^{a_i}.$$

Ko imamo D_P izbran, je funkcija f določena do konstante natančno. Ker je $\deg(D_Q) = \sum_i a_i = 0$, se vsaka konstanta v definiciji parjenja okrajša. Preverimo še kaj se zgodi, ko spremenimo izbiro D_P in D_Q. Naj bosta D'_P in D'_Q delitelja stopnje 0, katerih sum je zaporedoma enaka P in Q in za katera velja $\phi(D'_Q) = D'_Q$ in $\phi(D'_P) = D'_P$. Potem je

$$D'_P = D_P + \mathrm{div}(g) \;\text{ in }\; D'_Q = D_Q + \mathrm{div}(h)$$

za neki funkciji g in h. Po lemi 5.3.3 lahko predpostavimo, da sta g in h definirani nad $\mathbb{F}_q$. Velja tudi $\mathrm{div}(f') = nD'_P$ za neko funkcijo f' definirano nad $\mathbb{F}_q$.

Najprej predpostavimo, da D'_Q nima skupnih točk z D_P in D'_P, in da D'_P nima skupnih točk z D_Q. Ker je

$$\mathrm{div}(f') = \mathrm{div}(fg^n),$$

je $f' = cfg^n$ za neko konstanto c. Zdaj uporabimo f' in D'_Q za definicijo parjenja, ki ga bomo označili z $\langle ., .\rangle'_n$. Tako dobimo

$$\langle P, Q\rangle'_n = f'(D'_Q) = f(D'_Q)g(D'_Q)^n = f(D_Q)f(\mathrm{div}(h))g(D'_Q)^n.$$

Z uporabo Weilove recipročnosti 3.3.13 dobimo

$$\begin{aligned}\langle P,Q\rangle'_n &= f(D_Q)h(\mathrm{div}(f))g(D'_Q)^n \\ &= f(D_Q)h(D_P)^n g(D'_Q)^n.\end{aligned}$$

Iz $\phi(h(D_P)) = h(\phi(D_P)) = h(D_P)$ in podobno za $g(D'_Q)$ sklepamo, da sta $h(D_P)$ in $g(D'_Q)$ elementa $\mathbb{F}_q^*$. Posledično je

$$\langle P,Q\rangle'_n \equiv \langle P,Q\rangle_n \pmod{(\mathbb{F}_q^*)^n},$$

torej je parjenje neodvisno od izbire D_P in D_Q po modulu n-te potence.

Za splošen primer, ko dopustimo, da imajo D_P, D'_P in D_Q, D'_Q skupne točke, uporabimo lemo 5.3.2 za izbiro disjunktnih deliteljev D''_P in D''_Q, ki sta disjunktna vsem naštetim deliteljem. Potem je

$$\langle P,Q\rangle'_n \equiv \langle P,Q\rangle''_n \equiv \langle P,Q\rangle_n \pmod{(\mathbb{F}_q^*)^n}.$$

Tako smo dokazali, da je parjenje neodvisno od izbire D_P in D_Q po modulu n-te potence.

Naj bosta zdaj Q_1 in Q_2 dve točki in D_{Q_1} in D_{Q_2} pripadajoča delitelja. Potem je

$$D_{Q_1} + D_{Q_2} \sim (Q_1) - (\mathcal{O}) + (Q_2) - (\mathcal{O}) \sim (Q_1 + Q_2) - (\mathcal{O}),$$

kjer $\sim$ označuje ekvivalenco po modulu glavnih deliteljev. Zadnja ekvivalenca je posledica dejstva, da je preslikava sum homomorfizem grup. Posledično je

$$\langle P, Q_1 + Q_2\rangle_n = f(D_{Q_q})f(D_{Q_2}) = \langle P,Q_1\rangle_n\langle P,Q_2\rangle_n.$$

Parjenje je torej linearno v drugi spremenljivki.

Če sta $P_1, P_2 \in E(\mathbb{F}_q)[n]$ in D_{P_1}, D_{P_2} pripadajoča delitelja ter f_1, f_2 pripadajoči funkciji, potem je

$$D_{P_1} + D_{P_2} \sim (P_1) - (\mathcal{O}) + (P_2) - (\mathcal{O}) \sim (P_1 + P_2) - (\mathcal{O}).$$

Od tod sledi $D_{P_1+P_2} = D_{P_1} + D_{P_2}$ in

$$\mathrm{div}(f_1 f_2) = nD_{P_1} + nD_{P_2} = nD_{P_1+P_2},$$

zato za računanje parjenja uporabimo $f_1 f_2$. Enakost

$$\langle P_1 + P_2, Q\rangle_n = f_1(D_Q)f_2(D_Q) = \langle P_1,Q\rangle_n\langle P_2,Q\rangle_n$$

dokaže, da je parjenje linearno v prvi spremenljivki.

Neizrojenost parjenja bomo dokazali kasneje, ko bomo vpeljali ekvivalentno definicijo, pri kateri je neizrojenost lažje dokazljiva.

Ostane nam še modificirano Tate-Lichtenbaumovo parjenje. Ker je $\mathbb{F}_q^*$ ciklična grupa reda $q-1$ nam $(q-1)/n$-ta potenca porodi izomorfizem

$$\begin{array}{ccc}\mathbb{F}_q^*/(\mathbb{F}_q^*)^n & \to & \mu_n, \\ a & \mapsto & a^{(q-1)/n}.\end{array}$$

Tako lahko definiramo modificirano Tate-Lichtenbaumovo parjenje kot

$$\tau_n(P,Q) = \langle P,Q\rangle_n^{(q-1)/n}.$$

Lastnosti modificiranega Tate-Lichtenbaumovega parjenja τ_n tako sledijo iz lastnosti osnovnega Tate-Lichtenbaumovega parjenja. ■

Podobno kot pri Weilovem parjenju, imamo tudi za Tate-Lichtenbaumovo parjenje dve ekvivalentni definiciji. Zato si bomo v nadaljevanju ogledali alternativno definicijo, ter dokazali določne lastnosti in ekvivalenco obeh definicij.

Izrek 5.3.4. *Naj bo E eliptična krivulja nad $\mathbb{F}_q$ in n naravno število, ki deli $q-1$. Z $E(\mathbb{F}_q)[n]$ označimo elemente $E(\mathbb{F}_q)$, katerih red deli n. Naj bo $\mu_n = \{x \in \mathbb{F}_q^* : \ x^n = 1\}$. Izberimo $P \in E(\mathbb{F}_q)[n]$ in $Q \in E(\mathbb{F}_q)$, ter tak $R \in E(\overline{\mathbb{F}}_q)$, da je $nR = Q$. Z e_n bomo označili Weilovo parjenje in s ϕ q-ti Frobeniusov endomorfizem. Preslikava*

$$\begin{array}{rccc} \tau_n: & E(\mathbb{F}_q)[n] \times E(\mathbb{F}_q)/nE(\mathbb{F}_q) & \to & \mu_n \\ & (P,Q) & \mapsto & e_n(P, R-\phi(R)) \end{array}$$

je dobro definirano neizrojeno bilinearno parjenje.

Dokaz. Najprej bomo dokazali, da je τ_n dobro definiran in neodvisen od izbire R. Ker je $nR = Q \in E(\mathbb{F}_q)$, velja

$$\mathcal{O} = Q - \phi(Q) = n(R - \phi(R)),$$

torej je $R-\phi(R) \in E[n]$. Ker je tudi $P \in E[n]$, je Weilovo parjenje $e_n(P, R-\phi(R))$ dobro definirano. Recimo, da je $nR' = Q$ za drugo izbiro $R \neq R'$. Naj bo $T = R' - R$. Potem je $nT = Q - Q = \mathcal{O}$ in zato $T \in E[n]$. Od tod dobimo

$$\begin{array}{rcl} e_n(P, R' - \phi(R')) & = & e_n(P, R - \phi(R) + T - \phi(T)) \\ & = & e_n(P, R-\phi(R)) e_n(P,T)/e_n(P,\phi(T)). \end{array}$$

Ker pa velja $P \in E(\mathbb{F}_q)$ in $P = \phi(P)$, je tudi

$$e_n(P,\phi(T)) = e_n(\phi(P),\phi(T)) = \phi(e_n(P,T)) = e_n(P,T).$$

Torej τ_n ni odvisen od izbire R.

Ker je Q predstavnik odseka v $E(\mathbb{F}_q)/nE(\mathbb{F}_q)$, je potrebno dokazati, da je vrednost τ_n neodvisna od izbire predstavnika. Izberimo $Q' - Q = nU \in nE(\mathbb{F}_q)$, ter $nR = Q$ in $R' = R + U$. Potem je $nR' = Q'$ in velja

$$e_n(P, R' - \phi(R')) = e_n(P, R - \phi(R) + U - \phi(U)) = e_n(P, R - \phi(R)),$$

saj je $U = \phi(U)$ za vsak $U \in E(\mathbb{F}_q)$. Posledično τ_n ni odvisen od predstavnika odseka in je dobro definiran.

Bilinearnost τ_n v prvi spremenljivki sledi iz bilinearnosti Weilovega parjenja v prvi spremenljivki. Za bilinearnost v drugi spremenljivki Q pa predpostavimo, da je $nR_1 = Q_1$ in $nR_2 = Q_2$. Potem je $n(R_1 + R_2) = Q_1 + Q_2$ in

$$\begin{array}{rcl} \tau_n(P, Q_1 + Q_2) & = & e_n(P, R_1 + R_2 - \phi(R_1) - \phi(R_2)) \\ & = & e_n(P, R_1 - \phi(R_1)) e_n(P, R_2 - \phi(R_2)) \\ & = & \tau_n(P,Q_1)\tau_n(P,Q_2). \end{array}$$

■

V dokazu izreka 5.3.4 nismo dokazali neizrojenost parjenja. Za dokaz tega, bomo najprej dokazali, da sta obe definiciji ekvivalentni.

Izrek 5.3.5. *Parjenji τ_n definirani v izreku 5.3.4 in izreku 5.3.1 sta enaki.*

Dokaz. Privzemimo oznake izreka 5.3.4. Naj bo $Q \in E(\mathbb{F}_q)$ in $nR = Q$. Izberimo tako funkcijo g, da je

$$\mathrm{div}(g) = n(R) - (Q) - (n-1)(\mathcal{O}).$$

Naj g^ϕ označuje funkcijo dobljeno tako, da ϕ deluje na vse koeficiente racionalne funkcije g, tako da je $\phi(g(X)) = g^\phi(\phi(X))$ za vsak $X \in E(\overline{\mathbb{F}}_q)$. Ker je $\phi(Q) = Q$, velja

$$\mathrm{div}(g^\phi) = n(\phi(R)) - (Q) - (n-1)(\mathcal{O}).$$

Posledično je

$$\mathrm{div}(g/g^\phi) = n(R) - n(\phi(R)).$$

Izberimo $P \in E(\mathbb{F}_q)[n]$. Po lemi 5.3.2 obstaja tak delitelj D_P stopnje 0, da je $\mathrm{sum}(D_P) = P$, podpora D_P ne vsebuje točke $\mathcal{O}$, Q in R ter $\phi(D_P) = D_P$ (ϕ permutira točke v D_P).

Izberimo f z lastnostjo $\mathrm{div}(f) = nD_P$ kot v lemi 5.3.3, tako da je $f(\phi(R)) = \phi(f(R))$. Naj bodo $S = P$, $T = R - \phi(R)$, $D_S = D_P$, $D_T = (R) - (\phi(R))$, $F_S = f$ in $F_T = g/g^\phi$ kot v izreku 5.2.4. Ker ϕ potencira elemente $\overline{\mathbb{F}}_q$ na q-to potenco, velja

$$\begin{aligned}
\tau_n(P,Q) &= e_n(P, R - \phi(R)) \\
&= \frac{(g/g^\phi)(D_P)}{f((R) - (\phi(R))} \\
&= \phi\left(\tfrac{f(R)}{g(D_P)}\right)\left(\tfrac{g(D_P)}{f(R)}\right) \\
&= \left(\tfrac{f(R)}{g(D_P)}\right)^{q-1}.
\end{aligned}$$

Hkrati pa velja

$$\frac{f(R)^n}{f(Q)}\frac{f(\mathcal{O})}{f(\mathcal{O})^n} = f(\mathrm{div}(g)) = g(\mathrm{div}(f)) = g(D_P)^n.$$

Potem mora biti

$$\left(\frac{f(R)}{g(D_P)}\right)^n = \frac{f(Q)}{f(\mathcal{O})} f(\mathcal{O})^n.$$

Potenciranje zgornje enakosti na potenco $(q-1)/n$, nam da

$$\begin{aligned}
\tau_n(P,Q) &= \left(\tfrac{f(R)}{g(D_P)}\right)^{q-1} \\
&= \left(\tfrac{f(Q)}{f(\mathcal{O})}\right)^{(q-1)/n} f(\mathcal{O})^{q-1}.
\end{aligned}$$

Ker je $f^\phi = f$ in $\phi(\mathcal{O}) = \mathcal{O}$, je $f(\mathcal{O}) \in \mathbb{F}_q$. Torej je $f(\mathcal{O})^{q-1} = 1$. Če definiramo $D_Q = (Q) - (\mathcal{O})$, dobimo

$$\tau_n(P,Q) = f(D_Q)^{(q-1)/n}.$$

■

Preden dokažemo neizrojenost Tate-Lichtenbaumovega parjenja, potrebujemo še nekaj rezultatov povzetih po [152, poglavje 11].

Naj bo $n \in \mathbb{N}$ in naj bosta A in B končni Abelovi grupi reda n. Za bilinearno parjenje $\langle , \rangle : B \times A \to \mu_n$ pri fiksnem $a \in A$ lahko definiramo preslikavo

$$\begin{array}{rccc} \psi_a : & B & \to & \mu_n, \\ & b & \mapsto & \langle b, a \rangle. \end{array}$$

Tako definirana preslikava je homomorfizem. S $\mathrm{Hom}(B, \mu_n)$ bomo označili množico vseh homomorfizmov iz B v μ_n. Če na $\mathrm{Hom}(B, \mu_n)$ vpeljemo produkt s pravilom $(\alpha \cdot \beta)(b) = \alpha(b) \cdot \beta(b)$ za vsak $\alpha, \beta \in \mathrm{Hom}(B, \mu_n)$ in $b \in B$, dobimo Abelovo grupo.

Lema 5.3.6. *Če je B končna Abelova grupa reda n, velja $\#\mathrm{Hom}(B, \mu_n) = \#B$.* ■

Spomnimo se, da je po definiciji parjenje $\langle , \rangle : B \times A \to \mu_n$ neizrojeno v A, če iz $\langle b, a \rangle = 1$ za vsak $b \in B$ sledi $a = 0$.

Lema 5.3.7. *Naj bo parjenje $\langle , \rangle : B \times A \to \mu_n$ neizrojeno v A. Veljata naslednji trditvi:*

1. *Preslikava $A \to Hom(B, \mu_n)$ podana s pravilom $a \mapsto \psi_a$ je injektivna;*
2. *Če je $\#A = \#B$, potem je parjenje neizrojeno tudi v B.*

Dokaz. Naj bo ψ_a trivialen homomorfizem, tj. $\langle b, a \rangle = \psi_a(b) = 1$ za vsak $b \in B$. Iz neizrojenosti v A sledi, da je v tem primeru $a = 0$, kar dokaže točko 1. leme. Označimo

$$B_1 = \{b \in B : \ \langle b, a \rangle = 1 \ \forall a \in A\},$$

in za vsak $a \in A$ definirajmo

$$\begin{array}{rccc} \beta_a : & B/B_1 & \to & \mu_n, \\ & b \,(\mathrm{mod}\ B_1) & \mapsto & \langle b, a \rangle. \end{array}$$

Preslikava β_a je dobro definiran homomorfizem. Če je β_a trivialen homomorfizem, potem je $\langle b, a \rangle = 1$ za vsak $b \in B$, kar pomeni da je $a = 0$. Posledično je preslikava iz $A \to \mathrm{Hom}(B/B_1, \mu_n)$ injektivna in $\mathrm{Hom}(B/B_1, \mu_n)$ ima po lemi 5.3.6 red enak $\#B/\#B_1$. Ker pa je $\#A = \#B$, mora biti $\#B_1 = 1$, od koder sledi, da je $B_1 = 0$ in parjenje je neizrojeno tudi v B. ■

Velja tudi obrat točke 2. leme 5.3.7.

Lema 5.3.8. *Naj bo $\langle , \rangle : B \times A \to \mu_n$ neizrojeno parjenje v A in B. Potem je $\#A = \#B$ in $A \simeq \mathrm{Hom}(B, \mu_n)$, $B \simeq \mathrm{Hom}(A, \mu_n)$.* ■

Lema 5.3.9. *Naj bo M končna Abelova grupa in $\alpha : M \to M$ homomorfizem grup. Potem velja*

$$\#\ker(\alpha) = \#M/\#\alpha(M).$$

■

Naslednja lema je sicer tehnična, bo pa ključna v dokazu neizrojenosti Tate-Lichtenbaumovega parjenja.

Lema 5.3.10. *Naj bosta A in B končni Abelovi grupi reda n in*

$$\langle , \rangle : B \times A \to \mu_n,$$

bilinearno parjenje, ki je neizrojeno v obeh argumentih. Za podgrupo C grupe B definirajmo naslednjo preslikavo

$$\begin{array}{rccc} \psi: & A & \to & \prod_{c\in C} \mu_n, \\ & a & \mapsto & (\ldots, \langle c, a\rangle, \ldots). \end{array}$$

Potem je $\#\psi(A) = \#C$.

Dokaz. Ker je parjenje neizrojeno, je po lemi 5.3.9 $A \simeq \mathrm{Hom}(B, \mu_n)$. Po definiciji ψ je $\ker(\psi) = \{a \in A : \ \langle c, a\rangle = 1, \ \forall c \in C\}$. Če identificiramo A s $\mathrm{Hom}(B, \mu_n)$, je $\ker(\psi) = \{f \in \mathrm{Hom}(B, \mu_n) : \ f(C) = 1\}$. Homomorfizmi, ki preslikajo celoten C v 1, so natanko homomorfizmi iz B/C v μ_n. Množica takih homomorfizmov ima red $\#(B/C) = \#B/\#C$ in posledično je $\#\psi(A) = \#A/\#\ker(\psi) = \#A/\#(B/C) = \#C$, saj je $\#A = \#B$. ■

Rezultat leme 5.3.10 lahko zdaj uporabimo na eliptični krivulji E. Definirajmo naslednjo preslikavo

$$\begin{array}{rccc} \psi: & E[n] & \to & \displaystyle\prod_{P\in E(\mathbb{F}_q)[n]} \mu_n, \\ & Q & \mapsto & (\ldots, e_n(P, Q), \ldots). \end{array} \tag{5.11}$$

Lema 5.3.11. *Za q-ti Frobeniusov endomorfizem ϕ krivulje E je* $\ker(\psi) = (\phi - 1)E[n]$. ■

Zdaj lahko dokažemo, da je Tate-Lichtenbaumovo parjenje neizrojeno.

Dokaz. (Neizrojenost parjenja v izreku 5.3.1 in izreku 5.3.4.) Izberimo $Q \in E(\mathbb{F}_q)$ in jo zapišimo kot $Q = nR$, za nek $R \in E(\overline{\mathbb{F}}_q)$. Predpostavimo, da velja

$$\tau_n(P, Q) = e_n(P, R - \phi(R)) = 1, \quad \text{za vsak} \quad P \in E(\mathbb{F}_q)[n].$$

Potem je $R - \phi(R) \in \ker(\psi) = (\phi - 1)E[n]$, kjer je ψ preslikava definirana v (5.11). To pomeni, da obstaja taka točka $T \in E[n]$, da je $R - \phi(R) = \phi(T) - T$ oziroma, $\phi(R+T) = R+T$. Ker imajo točke, ki jih ϕ fiksira, koordinate v $\mathbb{F}_q$, velja $R+T \in E(\mathbb{F}_q)$. Ker je $Q = nR = n(R+T)$, je $Q \in nE(\mathbb{F}_q)$. To dokaže neizrojenost

$$\tau_n : E(\mathbb{F}_q)[n] \times E(\mathbb{F}_q)/nE(\mathbb{F}_q) \to \mu_n$$

v drugi spremenljivki. Ker pa imata po lemi 5.3.9 za $\alpha = [n]$ grupi $E(\mathbb{F}_q)[n]$ in $E(\mathbb{F}_q)/nE(\mathbb{F}_q)$ enak red, je po lemi 5.3.7 parjenje neizrojeno tudi v prvi spremenljivki. ■

Modificirano Tate-Lichtenbaumovo parjenje lahko razširimo na razširitve obsega $\mathbb{F}_q$.

Naj bo E eliptična krivulja nad $\mathbb{F}_q$, in n naravno število tuje k q, ki deli $\#E(\mathbb{F}_q)$. Naj bo k vključitvena stopnja $E(\mathbb{F}_q)$ glede na n. Potem je $\mu_n \subseteq \mathbb{F}^*_{q^k}$, in modificirano Tate-Lichtenbaumovo parjenje je definirano kot

$$\hat{\tau}_n(P, Q) = \langle P, Q\rangle_n^{(q^k-1)/n}. \tag{5.12}$$

Za tako definirano modificirano Tate-Lichtenbaumovo parjenje velja naslednja trditev.

Trditev 5.3.12. *Za naravni števili n in N kjer n deli N velja*

$$\langle P, Q\rangle_N^{(q^k-1)/N} = \langle P, Q\rangle_n^{(q^k-1)/n}$$

Dokaz. Naj bo D delitelj stopnje 0 ekvivalenten $(Q) - (\mathcal{O})$. Po izreku 4.2.8 obstaja funkcija g nad $\mathbb{F}_q$, za katero je $\mathrm{div}(g) = n(P) - n(\mathcal{O})$. Potem za $h = N/n$ velja $\mathrm{div}(g^h) = N(P) - N(\mathcal{O})$ in posledično

$$\langle P, Q\rangle_N^{(q^k-1)/N} = g^h(D)^{(q^k-1)/N} = g(D)^{(q^k-1)/n} = \langle P, Q\rangle_n^{(q^k-1)/n}.$$

■

5.4 Računanje parjenj

Zdaj ko smo definirali in spoznali lastnosti osnovnih primerov parjenj na eliptičnih krivuljah, bomo predstavili še algoritem za računanje le teh. Algoritem se po avtorju imenuje Millerjev algoritem [105] in je bil v osnovi narejen za računanje Weilovega parjenja. Uporablja pa se tudi za računanje Tate-Lichtenbaumovega parjenja in njunih izpeljank. Glavna ideja algoritma je konstruirati funkcijo f_P, katere delitelj bo imel naslednjo obliko

$$\mathrm{div}(f_P) = n(P) - n(\mathcal{O}). \tag{5.13}$$

Za generiranje take funkcije po korakih je Miller uporabil metodo podvoji in seštej. Na i-tem koraki generiramo i-to Millerjevo funkcijo, ki je na n-tem koraku enaka f_P.

Definicija 5.4.1. Naj bo E eliptična krivulja nad obsegom K. Pri dani točki $P \in E(K)$ ter $i \in \mathbb{N}$ je **Millerjeve funkcija** $f_{i,P} \in K(E)$ funkcija z deliteljem $\mathrm{div}(f_{i,P}) = i(P) - (iP) - (i-1)(\mathcal{O})$.

Če je $f_{1,P} = 1$, bo $f_{n,P} = f_P$ funkcija z želeno lastnostjo (5.13). Obstoj funkcije je zagotovljen z lastnostmi deliteljev v izreku 4.2.8. Za Millerjevo funkcijo pa velja še dodatna lastnost, ki bo ključna v algoritmu za računanje parjenj.

Lema 5.4.2. *Izberimo $i, j \in \mathbb{N}$ in $P \in E(K)$. Naj bo ℓ enačba premice skozi točki iP in jP in v enačba navpične premice skozi točko $iP + jP$. Potem velja*

$$f_{i+j,P} = f_{i,P} f_{j,P} \frac{\ell}{v}. \tag{5.14}$$

Dokaz. Po definiciji seštevanja v E je tretja presečna točka ℓ in E enaka $-(i+j)P$. Podobno v seka E v točkah $(i+j)P$, $-(i+j)P$ in $\mathcal{O}$. Izračunajmo

$$\begin{aligned}
\mathrm{div}(f_{i,P} f_{j,P} \tfrac{\ell}{v}) &= \mathrm{div}(f_{i,P}) + \mathrm{div}(f_{j,P}) + \mathrm{div}(\ell) - \mathrm{div}(v) \\
&= i(P) - (iP) - (i-1)(\mathcal{O}) \\
&\quad + j(P) - (jP) - (j-1)(\mathcal{O}) \\
&\quad + (iP) + (jP) + (-(i+j)P) - 3(\mathcal{O}) \\
&\quad - ((i+j)P) - (-(i+j)P) + 2(\mathcal{O}) \\
&= (i+j)(P) - ((i+j)P) - (i+j-1)(\mathcal{O}) \\
&= \mathrm{div}(f_{i+j,P}).
\end{aligned}$$

■

Te formule lahko najhitreje uporabimo v primeru $j = 1$ (seštevanje) in $j = i$ (podvajanje). Millerjev algoritem uporablja verigo seštevanj za nP za izračun $f_{n,P} = f_P$. Ker nas zanima vrednost $f_{n,P}$ na deliteljju, izračunamo tudi vse vmesne Millerjeve funkcije na deliteljju oblike $D = (Q + S) - (S)$.

Algoritem 5.4.1 Millerjev algoritem za računanje Tate-Lichtenbaumovega parjenja

Vhodni podatki: $P, Q \in E(K)$, kjer je red P enak n.
Rezultat: $\langle P, Q \rangle_n$.

1. Izberimo primerno točko $S \in E[n] - \{\mathcal{O}, P, -Q, P - Q\}$;
2. $Q' \leftarrow Q + S$;
3. $T \leftarrow P$;
4. $m \leftarrow \lfloor \log_2(n) \rfloor - 1$;
5. $f \leftarrow 1$;
6. **while** $m \geq 0$ **do**
   (a) izračunaj premici ℓ in v za podvajanje točke T;
   (b) $T \leftarrow 2T$;
   (c) $f \leftarrow f^2 \cdot \frac{\ell(Q')}{v(Q')} \cdot \frac{v(S)}{\ell(S)}$;
   (d) **if** m-ti bit od n enak 1 **then**
      i. izračunaj premici ℓ in v za seštevanje $T + P$;
      ii. $T \leftarrow T + P$;
      iii. $f \leftarrow f \cdot \frac{\ell(Q')}{v(Q')} \cdot \frac{v(S)}{\ell(S)}$;
   (e) **end if**
   (f) $m \leftarrow m - 1$;
7. **end while**
8. **Vrni** f.

Eden izmed načinov za izbiro primerne točke S je naključna točka v $E(K)$. V primerih, ko je n velik, je algoritem deterministično pri pogoju, da je $S = iP$, kjer binarni zapis i ni del binarnega zapisa n.

Lahko se zgodi, da Millerjev algoritem ne vrne rezultata. To je v primeru, ko imata vmesni premici ℓ ali v ničlo v točki Q' ali S. Vendar pa se v protokolih, ki temeljijo na parjenjih to ne zgodi, saj običajno velja $P \in E(\mathbb{F}_q)$ in $Q \notin E(\mathbb{F}_q)$. V tem primeru so vse ničle ℓ in v v grupi generirani s točko P in če vzamemo $S = Q$, se tak scenarij ne zgodi.

Vrstica 5.d.iii. algoritma se poenostavi v $\ell = (x - x_P)$ in $v = 1$ v zadnji iteraciji, saj je v tem primeru $T = -P$. Število vseh iteracij celotnega algoritma je $\log_2(n)$, torej je operacij podvajanja $\log_2(n)$. Število seštevanj (10 in 12 vrstica) je enaka polovici Hammingove uteži števila n. Torej je algoritem polinomski.

Predstavljeni algoritem je splošen Millerjev algoritem za računanje Tate-Lichtenbaumovega parjenja in se lahko uporabi tudi za računanje Weilovega parjenja in njunih izpeljank. Sam algoritem je možno optimizirati glede na krivuljo in obseg. Več o optimizaciji algoritma je na voljo v [8, 32, 133, 134].

Primer. Naj bo $E : y^2 = x^3 + 1$ nad $\mathbb{F}_{101}$. Potem je $\#E(\mathbb{F}_{101}) = 101 + 1 = 2 \cdot 3 \cdot 17$. Za $n = 17$ je vključitvena stopnja $k = 2$. Zdaj lahko zapišemo $\mathbb{F}_{101^2} = \mathbb{F}_{101}(\phi)$, kjer je $\phi = -2$. Izberimo točki $P = (87, 61)$ reda 17 in $Q = (48, \phi)$ reda 102. Naj bo $D = (2Q) - (Q)$. Izračunajmo zdaj naslednje vrednosti:

i	1	2	4	8	16	17
$f_i(D)$	1	$52 + 56\phi$	$53 + 3\phi$	$46 + 18\phi$	$22 + 43\phi$	$74 + 62\phi$

Torej je

$$\langle P, Q \rangle_{17} = 74 + 62\phi,$$

kar potenciramo na $(101^2 - 1)/17 = 600$ in dobimo $93 + 25\phi \in \mu_{17}$. •

5.5 Distorzijske preslikave

Ena izmed zanimivih posledic parjenj so distorzijske preslikave, ki ohranjajo določene lastnosti.

Definicija 5.5.1. Izberimo eliptično krivuljo nad obsegom $\mathbb{F}_q$ in praštevilo r, ki deli $\#E(\mathbb{F}_q)$. Naj bo $e : E[r] \times E[r] \to \mu_r$ neizrojeno bilinearno parjenje in naj bo $P \in E(\mathbb{F}_q)[r]$. **Distorzijska preslikava** glede na E, r, e in P je tak endomorfizem ψ, za katerega velja $e(P, \psi(P)) \neq 1$.

O obstoju distorzijskih preslikav nam veliko pove naslednja lema.

Lema 5.5.2. *Naj ima $P \in E(\mathbb{F}_q)$ praštevilski red r in naj bo $k > 1$. Predpostavimo, da $E(\mathbb{F}_q)$ nima točk reda r^2. Izberimo endomorfizem ψ krivulje E, da velja $\psi(P) \notin rE(\mathbb{F}_{q^k})$. Potem je ψ distorzijska preslikava.*

Skica dokaza. Ker je ψ endomorfizem, je red $\psi(P)$ ali r ali 1. Ker pa $\psi(P) \notin E(\mathbb{F}_q)$, red $\psi(P)$ ne more biti enak 1. Torej sta $P, \psi(P)$ netrivialni in neodvisni r-torzijski točki na krivulji E in ker ni točk z redom r^2, velja $\psi(P) \notin rE(\mathbb{F}_{q^k})$. Ker je e neizrojeno bilinearno parjenje, velja $e(P, P) = 1$ in posledično je $e(P, \psi(P)) \neq 1$. ■

Verheul je leta 2004 dokazal [149], da za vsako supersingularno eliptično krivuljo obstaja distorzijska preslikava. Velja pa tudi obrat, zajet v naslednjem izreku.

Izrek 5.5.3. *Naj bo E eliptična krivulje nad obsegom $\mathbb{F}_q$, ki ima distorzijsko preslikavo. Potem je E supersingularna.*

Skica dokaza. Naj bo ψ endomorfizem, ki preslika $P \in E(\mathbb{F}_q)$ v $\psi(P) \notin E(\mathbb{F}_q)$. Za q-ti Frobeniusov endomorfizem ϕ je $\phi(P) = P$ in $\phi(\psi(P)) \neq \psi(P)$. Posledično $\psi \circ \phi \neq \phi \circ \psi$ v grupi endomorfizmov $\mathrm{End}(E)$, zato je $\mathrm{End}(E)$ nekomutativna in E je supersingularna krivulja. ■

Ker je v primeru supersingularnih krivulj P definirana nad majhnim obsegom, imamo učinkovito reprezentacijo za vse točke eliptične krivulje in posledično je Millerjev algoritem bolj učinkovit. Zaradi tega so supersingularne krivulje posebej primerne za parjenja.

Poglavje 6

UPORABA PARJENJ V KRIPTOGRAFIJI

V nadaljevanju si bomo ogledali nekaj primerov uporabe parjenj v kriptografiji. Začeli bomo s prvim primerom uporabe parjenj, to je napadom na diskretni logaritem, nato bomo nadaljevali s shemami za šifriranje in podpisovanje na podlagi identitete in tripartitnim protokolom. Zaključili bomo z različnimi primeri shem za podpise, ki uporabljajo parjenja. Več o uporabi parjenj je na voljo v [157, 158].

6.1 MOV/Frey Rück napad na ECDLP

Pomembna uporaba parjenj v kriptografiji je v pretvorbi diskretnega logaritma na eliptičnih krivuljah v diskretni logaritem v končnih obsegih. Motivacija za tak pristop je v index-calculus algoritmu za računanje diskretnega logaritma v končnih obsegih [83], katerega zahtevnost je podeksponentna. Napad z Weilovim parjenjem so prvi opisali Menezes, Oakamoto in Vanstone (MOV) [101], napad s Tate-Lichtenbaumovim parjenjem sta opisala Frey in Rück [51]. V nadaljevanju bomo opisali splošni algoritem, glej 6.1.1.

Naj bo E eliptična krivulja nad obsegom $\mathbb{F}_q$, naj bosta $P, Q \in E[n]$, kjer je $\gcd(n, q) = 1$ in n praštevilo in naj bo $Q = \lambda P$, za nek $\lambda \in \mathbb{N}$. Naj $e(P, Q)$ označuje bilinearno parjenje (Tate-Lichtenbaum, Weil).

Obstoja števila k v koraku 1 tega algoritma nam zagotavlja trditev 4.7.2. Točko S v koraku 3 dobimo z naključno izbiro točke. Take točke obstajajo po definiciji parjenja 2.1 in verjetnost, da bo tako izbrana točka zadoščala, je velika [16].

Večina korakov v tem algoritmu je računsko enostavnih, z izjemo reševanja diskretnega logaritma (računanje λ, $\zeta_1^\lambda = \zeta_2$ v $\mathbb{F}_{q^k}^*$) v koraku 6. To se naredi z index-calculus metodo, ki je podeksponentna glede na velikost binarnega zapisa števila q^k. Napad je uspešen le, če je vrednost parametra k majhna.

Algoritem 6.1.1 MOV/Frey Rück napad na ECDLP

Vhodni podatki: krivulja E nad obsegom $\mathbb{F}_q$, kjer je q potenca praštevila,$P, Q \in E[n]$, n tako praštevilo $\gcd(n, q) = 1$, obseg $\mathbb{F}_q$, $Q = \lambda P$ za neznano vrednost $\lambda \in \mathbb{N}$.
Rezultat: diskretni logaritem λ.

1. Naj bo $k \in \mathbb{N}$ najmanjše tako število, da n deli $q^k - 1$;
2. Konstruiraj obseg $\mathbb{F}_{q^k}$;
3. Poišči tako točko $S \in E(\mathbb{F}_{q^k})$, za katero velja $e(P, S) \neq 1$;
4. Izračunaj $\zeta_1 \leftarrow e(P, S)$;
5. Izračunaj $\zeta_2 \leftarrow e(Q, S)$;
6. Poišči λ tak, da je $\zeta_1^\lambda = \zeta_2$ v $\mathbb{F}_{q^k}^*$;
7. **Vrni** λ.

6.2 Šifriranje na podlagi identitete

Pri uporabi kriptografije z javnimi ključi, oseba A z javnim ključem osebe B šifrira sporočilo in ga pošlje osebi B, ki ga s pripadajočim zasebnim ključem odšifrira. Oseba A mora pri tem imeti zagotovilo, da v resnici poseduje pravi javni ključ, ki pripada osebi B. Tako zagotovilo prepreči napadalcu C, da se predstavlja osebi A kot oseba B in tako prestreza in odšifrira sporočila namenjena osebi B (ang. man in the middle attack).

Pri reševanju problema se ponavadi uporabi certificirana avtoriteta oziroma agencija za overjanje (ang. certified authority - CA), ki je odgovorna za generiranje certifikatov oziroma digitalnih potrdil za javne ključe. Tak certifikat $\mathrm{Cert}(B)$ za osebo B vsebuje podatke o identiteti ID_B osebe B in javni ključ PK_B osebe B skupaj z digitalnim podpisom $\mathrm{sgn}_{\mathrm{CA}}$ vseh teh podatkov

$$\mathrm{Cert}(B) = (\mathrm{ID}_B, \mathrm{PK}_B, \mathrm{sgn}(\mathrm{ID}_B, \mathrm{PK}_B)_{\mathrm{CA}}).$$

Tako lahko vsaka entiteta, ki poseduje javni ključ CA, preveri podpis v certifikatu in se na podlagi tega prepriča, da poseduje javni ključ osebe, kateri želi poslati šifrirano sporočilo.

Čeprav je zgoraj opisana rešitev na prvi pogled enostavna, pa je v praksi drugače. Tako recimo oseba B ne ve kje dobi certifikat osebe A, poleg tega pa mora imeti zagotovilo, da je certifikat še veljaven (ni preklican ali ni pretekel).

Leta 1984 je Shamir [128] predstavil princip šifriranja, ki temelji na identiteti uporabnika (ang. identity based encryption), z namenom, da poenostavi probleme z upravljanjem certifikatov. Tako predlaga, da je javni ključ osebe A sestavljen iz podatkov, ki izkazujejo identiteto oseba A - ID_A (e-mail, naslov,...). Poleg tega je predlagal uvedbo zaupanja vredne tretje osebe (ang. trusted third party - TTP), ki z uporabo svojega privatnega ključa generira privatni ključ osebe A iz ID_A in ga varno dostavi osebi A. Vsak drugi uporabnik, ki bi želel varno komunicirati z osebo A, bi šifriral sporočilo z ID_A in javnim ključem TTP Za razliko od sistema s certifikati, lahko pošlje osebi A sporočilo še preden

oseba A generira svoj privatni ključ pri TTP. Problem veljavnosti, poteka ali preklica se lahko reši s pomočjo dodatnih časovnih podatkov.

Boneh-Franklin-ova shema za šifriranje

Leta 2001 sta Boneh in Franklin [18] predlagala prvo praktično šifrirno shemo, ki temelji na identiteti uporabnika. Predlagana shema uporablja bilinearno parjenje $e : G_1 \times G_1 \to G_2$, na paru grup (G_1, G_2), na katerih je BDHP težko izračunljiv in kriptografski zgoščevalni funkciji:

$$H_1 : \{0,1\}^* \to G_1 \setminus \{\infty\},$$

$$H_2 : G_2 \to \{0,1\}^{\ell},$$

kjer je ℓ dolžina čistopisa v bitih. TTP-jev zasebni ključ je naključno izbrano naravno število $t \in [1, n-1]$, javni ključ pa $T = tP$, kjer je P naključno izbran generator grupe G_1. Predpostavlja se še, da lahko vsi uporabniki pridobijo avtenticirano kopijo javnega ključa T. Ko oseba A zahteva svoj privatni ključ d_A, TTP na podlagi ID_A generira $d_A = tH_1(\mathrm{ID}_A)$, in ga varno dostavi osebi A. Algoritma za šifriranje in dešifriranje sta predstavljena spodaj.

Algoritem 6.2.1 Šifriranje

Vhodni podatki: čistopis $m \in \mathcal{M}$, javni ključ ID_A osebe A, javni ključ T TTP, generator P grupe G_1.
Rezultat: tajnopis $c = (U, V)$.

1. Izračunaj $Q_{\mathrm{ID}_A} = H_1(\mathrm{ID}_A) \in G_1^*$;
2. Izberi naključno število $r \in \mathbb{Z}_q^*$;
3. Izračunaj tajnopis:
$$c = \left(rP, m \oplus H_2(g_{\mathrm{ID}_A}^r)\right),$$
kjer je $g_{\mathrm{ID}_A} = e(Q_{\mathrm{ID}_A}, T) \in G_2^*$.

Algoritem 6.2.2 Dešifriranje

Vhodni podatki: tajnopis $c = (U, V) \in \mathcal{C}$, privatni ključ $d_{\mathrm{ID}_A} \in G_1^*$.
Rezultat: dešifriran čistopis m.

1. Izračunaj:
$$m = V \oplus H_2(e(d_{\mathrm{ID}_A}, U)).$$

Napadalec, ki bi rad prestregel in dešifriral sporočilo m iz para $c = (U, V)$ mora znati izračunati $e(Q_{\mathrm{ID}_A}, T)^r$ pri znanih vrednostih podatkov $(P, Q_{\mathrm{ID}_A}, T, U)$, kar je ekvivalentno reševanju bilinearnega Diffie-Hellmanovega problema (BDHP), definiranega v definiciji 2.3.

Pri predpostavki, da je BDHP težko izračunljiv na grupah G_1 in G_2 in da sta H_1 ter H_2 naključna oraklja, je tako definirana shema semantično varna [18]. Vendar pa shema ni odporna na napade z izbranim tajnopisom (ang. choosen-chiperattack), kjer napadalec za vsak izbran tajnopis, razen za tistega, ki ga napada, dobi čistopis. [100, 18]. Da bi shemo naredili odporne na take napade, moramo dodati kriptografski zgoščevalni funkciji:

$$H_3 : \{0,1\}^* \to [1, n-1],$$

$$H_4 : \{0,1\}^l \to \{0,1\}^l.$$

Spremenjena algoritma za šifriranje in dešifriranje sta spodaj.

Algoritem 6.2.3 Šifriranje

Vhodni podatki: čistopis $m \in \mathcal{M}$, javni ključ ID_A osebe A, javni ključ T TTP, generator P grupe G_1.
Rezultat: tajnopis $c = (U, V, W)$.

1. Izračunaj $Q_{\mathrm{ID}_A} = H_1(\mathrm{ID}_A) \in G_1^*$;
2. Izračunaj naključni $\rho \in \{0,1\}^n$;
3. Izračunaj $r = H_3(\rho, m)$;
4. Izračunaj $g_{\mathrm{ID}_A} = e(Q_{\mathrm{ID}_A}, T) \in G_2$;
5. Izračunaj tajnopis:

$$c = \left(rP, \rho \oplus H_2(g_{\mathrm{ID}_A}^r), m \oplus H_4(\rho)\right).$$

Algoritem 6.2.4 Dešifriranje

Vhodni podatki: tajnopis $c = (U, V, W) \in \mathcal{C}$, privatni ključ $d_{\mathrm{ID}_A} \in G_1^*$, generator P grupe G_1
Rezultat: dešifriran čistopis m.

1. Izračunaj $V \oplus H_2(e(d_{\mathrm{ID}_A}, U)) = \rho$;
2. Izračunaj $W \oplus H_4(\rho) = m$;
3. Izračunaj $r = H_3(\rho, m)$;
4. **if** $U \neq rP$ **then**
   Zavrni sporočilo;
5. **else**
   m je dešifrirani čistopis tajnopisa c;
6. **end if**

6.3 Tripartitni protokol za dogovor o ključu

Dobro znan primer v kriptografiji je Diffie-Hellmanov protokol za dogovor o ključu med dvema entitetama. Namen tega je, da si entiteti udeleženi v pogovor na varen način izmenjata sejni ključ preko kanala, ki ga lahko spremlja tudi napadalec. Osnovni algoritem je sledeči:

Algoritem 6.3.1 Osnovni protokol za dogovor o ključu

Vhodna podatka: red n grupe G , P generator grupe G.
Rezultat: dogovorjen ključ $K = abP$.

A:

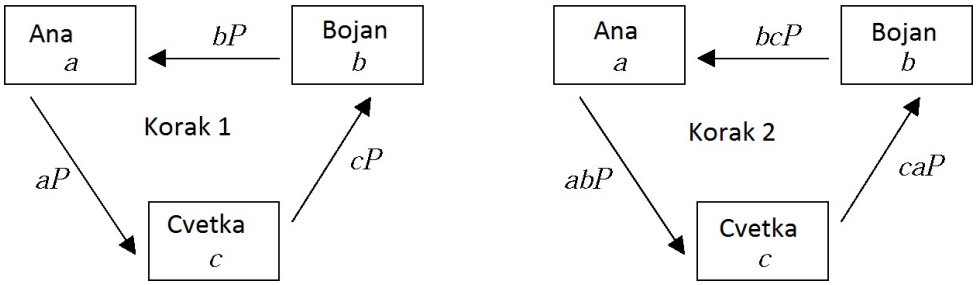
1. Izbere naključno število $a \in [1, n-1]$;
2. Pošlje vrednost aP entiteti B.

B:

1. Izbere naključno število $b \in [1, n-1]$;
2. Pošlje vrednost bP entiteti A.

Skupni sejni ključ, ki ga lahko izračunata obe entiteti, je $K = abP$.

Morebitni napadalec mora izračunati K pri vrednostih aP, bP in P, kar je ravno Diffie-Hellmanov problem, ki smo ga predstavili v poglavju 2. Na zgornji protokol lahko gledamo kot na eno-koračni protokol, saj obe entiteti lahko izračunata svoji vrednosti neodvisno in jih v enem koraku pošljeta drug drugi. Protokol lahko razširimo tudi na tri entitete, kjer pa se izmenjava podatkov izvede v dveh korakih, kot je razvidno iz slike 6.1.



Slika 6.1: Dogovor o ključu v dveh korakih

V zgornjem protokolu je skrivni sejni ključ $K = abcP$. Protokol je varen, če je problem izračunati vrednost $abcP$ pri znanih vrednostih P, aP, bP, cP, abP, bcP, caP težak (enakovreden DH). Pri tripartitnem protokolu se pojavi vprašanje, ali obstaja protokol, s katerim bi izmenjavo ključa dosegli v enem krogu in ki bi bil varen pred napadalcem. Problem je leta 2000 rešil Joux [68] s pomočjo bilinearnih parjenj. V nadaljevanju bomo

na kratko predstavili njegov rahlo modificiran protokol [149]. Tripartitini protokol za izmenjavo ključa v enem krogu uporablja bilinearno parjenje e na paru grup (G_1, G_2) za katerega je BDHP težko izračunljiv in je opisan v 6.3.2.

Algoritem 6.3.2 Tripartitni protokol za dogovor o ključu s parjenjem

---

Vhodni podatki: red n grupe G_1, element P generator grupe G_1, parjenje $e : G_1 \times G_1 \to G_2$ na paru grup (G_1, G_2).
Rezultat: dogovorjen ključ $K = e(P, P)^{abc}$.

A:

1. Izbere naključno število $a \in [1, n-1]$;
2. Pošlje vrednost aP entiteti B in entiteti C.

B:

1. Izbere naključno število $b \in [1, n-1]$;
2. Pošlje vrednost bP entiteti A in entiteti C.

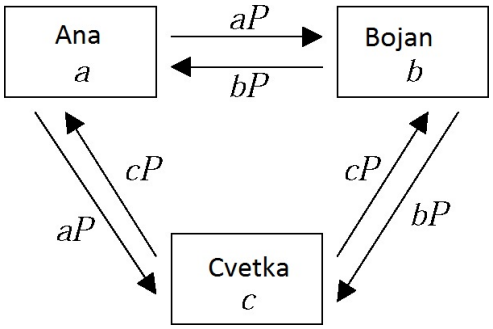
C:

1. Izbere naključno število $c \in [1, n-1]$;
2. Pošlje vrednost cP entiteti A in entiteti B.

Skupni sejni ključ, ki ga lahko izračunajo vse entitete je

$$K = e(bP, cP)^a = e(aP, cP)^b = e(aP, bP)^c = e(P, P)^{abc}.$$

Napadalec, ki pri danih podatkih P, aP, bP, cP, n, e želi izračunati ključ K, mora rešiti BDHP. Protokol je viden tudi sliki 6.2.



Slika 6.2: Dogovor o ključu v enem koraku s parjenjem.

6.4 Podpisi s parjenjem

Večina shem za podpise, ki temeljijo na diskretnem algoritmu, kot npr. DSA [39], so variante El-Gamalove sheme za podpise [44]. V takih shemah so podpisi ponavadi sestavljeni iz para celih števil po modulu n, kjer je n red uporabljene grupe $G = \langle P \rangle$. S parjenjem na eliptičnih krivuljah pa lahko konstruiramo tudi drugačne podpise, ki jih bomo predstavili v naslednjih razdelkih.

6.4.1 Podpisi na podlagi identitete

Kmalu po objavi Boneh-Franklinove sheme za šifriranje na podlagi identitete uporabnika, so se pojavile tudi sheme za podpisovanje, ki so temeljile na identiteti uporabnika [33, 63, 64, 117]. Tu bomo predstavili samo eno izmed njih in sicer shemo, ki sta jo predstavila Cha in Cheon [33].

Podobno kot sheme za šifriranje na podlagi identitete, tudi ta shema uporablja bilinearno parjenje $e : G_1 \times G_1 \to G_2$ na grupah G_1 in G_2 praštevilskega reda q, naključno izbran generator $P \in G_1$, javni ključ $T = tP$, kjer je $t \in \mathbb{Z}_q^*$ izbran naključno, zgoščevalni funkciji $H_1 : \{0,1\}^* \to G_1^*$ in $H_2 : \{0,1\}^* \times G_1 \to \mathbb{Z}_q$, ter privatni ključ osebe A, ki je enak $d_A = tH_1(\mathrm{ID}_A)$. Algoritma za podpisovanje in preverjanje podpisa sta opisana v 6.4.1 in 6.4.2 respektivno.

Algoritem 6.4.1 Podpisovanje na podlagi identitete

Vhodni podatki: sporočilo $m \in \{0,1\}^*$, ID_A in d_A.
Rezultat: podpis (U, V).

1. Izberi naključen $s \in \mathbb{Z}_q$;
2. Izračunaj $U = sH_1(\mathrm{ID}_A)$;
3. Izračunaj $h = H_2(m, U)$.
4. Izračunaj $V = (s + h)d_A$;

Podpis je par (U, V).

6.4.2 Kratki podpisi

Boneh, Lynn in Shacham [23] so predlagali prvo shemo, pri kateri je podpis sestavljen iz enega samega elementa grupe G. Pri tem so uporabili bilinearno parjenje $e : G_1 \times G_1 \to G_2$, kjer imata grupi G_1 in G_2 praštevilski red q in za katerega je DHP v G_1 težko izračunljiv. Poleg parjenja na grupah uporabijo še zgoščevalno funkcijo $H : \{0,1\}^* \to G_1 \setminus \{\infty\}$ in naključni generator P grupe G_1. Privatni ključ osebe A je vrednost a, kjer je $a \in [1, q-1]$ izbran naključno, javni ključ je aP. Algoritma za podpisovanje in preverjanje podpisa sta v 6.4.3 in 6.4.4 respektivno.

Algoritem 6.4.2 Preverjanje podpisa na podlagi identitete

Vhodni podatki: podpis $c = (U, V)$, identiteta ID_A osebe A.
Rezultat: veljavnost podpisa.

1. Izračunaj $e(P, V)$;
2. Izračunaj $e(T, U + hH_1(\mathrm{ID}_A))$;
3. **if** $e(T, U + hH_1(\mathrm{ID}_A)) = e(P, V)$ **then**
   Podpis je veljaven;
4. **else**
   Podpis ni veljaven.
5. **end if**

Algoritem 6.4.3 Podpisovanje - kratki podpis

Vhodni podatki: sporočilo $m \in \{0,1\}^*$, generator P grupe G_1 reda q, naključno izbrano število $a \in [1, q-1]$.
Rezultat: podpis S.

1. Izračunaj $M = H(m) \in G_1 \setminus \{\infty\}$;
2. Izračunaj $S = aM$.

Podpis sporočila m je $S \in G_1$.

Algoritem 6.4.4 Preverjanje kratkega podpisa

Vhodni podatki: generator P grupe G_1, javni ključ aP, parjenje e na paru grup G_1 in G_2, sporočilo m, podpis S.
Rezultat: veljavnost podpisa.

1. Izračunaj $M = H(m)$
2. **if** $e(P, S) = e(aP, M)$ **then**
   Podpis je veljaven;
3. **else**
   Podpis ni veljaven.
4. **end if**

6.4.3 Agregatni podpisi

Veliko aplikacij uporablja različne podpise različnih entitet. Kot primer si lahko ogledamo infrastrukturo javnih ključev globine ℓ, pri kateri vsakemu uporabniku priredimo verigo ℓ certifikatov, ki vsebuje ℓ podpisov ℓ certifikatnih agencij na ℓ različnih certifikatih. Podoben primer je recimo varen BGP protokol [75], v katerem vsak usmerjevalnik prejme seznam ℓ podpisov za testiranje določene poti v mreži dolžine ℓ. Usmerjevalnik nato podpiše svoj segment v poti in pošlje novi seznam $\ell+1$ podpisov naslednjemu usmerjevalniku. Posledično je število podpisov v sporočilu usmerjevalnikov linearno odvisno od števila usmerjevalnikov na poti. V obeh zgornjih primerih bi veliko pridobili, če bi namesto verige podpisov potrebovali samo enega.

Agregatni podpisi omogočajo reševanje problema opisanega v zgornjih dveh primerih. Naj bo ℓ število uporabnikov, vsak s svojim parom javnega in privatnega ključa (P, a_iP). Uporabnik u_i podpiše sporočilo m_i, da dobi podpis μ_i. Javni algoritem za agregatni podpis vzame kot vhodne podatke vse podpise $\mu_i, i = 1, \ldots, \ell$, rezultat algoritma pa je skrčen podpis μ. Vsak lahko ustvari agregatni podpis na ℓ podpisih, še več, agregatni podpisi se lahko kreirajo tudi inkrementno, tj. podpisa μ_X in μ_Y se lahko skrčita v podpis μ_{XY}, ki se lahko potem skupaj s podpisom μ_Z skrči v podpis μ_{XYZ}. Podobno algoritem za preverjanje podpisa vzame za vhodne podatke javne ključe uporabnikov $P_1, \ldots, P_\ell$ sporočila $m_1, \ldots, m_\ell$ in agregatni podpis μ ter preveri ali je le ta veljaven. Podpis bo veljaven, če so bili vhodni podatki pri generiranju agregatnega podpisa μ vsi $\mu_1, \ldots \mu_\ell$.

Agregatni podpisi, ki so jih predstavili Boneh, Gentry, Lynn, Shachan [19], uporabljajo bilinearna parjenja na grupah G_1, G_2, pri katerem je DH težko izračunljiv na G_1. Naj bo $\mathcal{U}$ množica uporabnikov. Vsak uporabnik $u \in \mathcal{U}$ ima par ključev za podpisovanje (P, a_uP). Želimo kreirati agregatni podpis za skupino uporabnikov $U \subseteq \mathcal{U}$. Vsak posamezni uporabnik $u \in \mathcal{U}$ kreira podpis μ_u na sporočilu m_u lastne izbire. Vsi podpisi μ_u bodo združeni v en agregatni podpis μ. Entiteta, ki izračuna agregatni podpis, je lahko različna od uporabnikov v množici U in ni nujno potrjena (ang. trusted) s strani uporabnikov. Imeti mora le dostop do javnih ključev uporabnikov v skupini U in njihovih podpisov sporočil μ_u. Algoritem ima lastnost, da lahko pri preverjanju podpisa μ skupaj z identitetami uporabnikov in sporočili m_u preverimo, ali je vsak uporabnik zares podpisal svoje sporočilo m_u. Algoritma za posamezen podpis in preverjanje posameznega podpisa sta enaka kot pri kratkih podpisih, 6.4.3 in 6.4.4 respektivno. Algoritma za kreiranje in preverjanje agregatnega podpisa pa sta predstavljena v v 6.4.5 in 6.4.6 respektivno.

Algoritem 6.4.5 Kreiranje agregatnega podpisa

Vhodni podatki: uporabniki $U \subseteq \mathcal{U}$, $u_i \in U, i = 1, \ldots, \ell =\mid U \mid$, sporočila $m_i \in \{0,1\}^*$.

Rezultat: agregatni podpis.

1. Vsak uporabnik $u_i \in U$ generira podpis $\mu_i = a_iH(m_i) \in G_1$ na sporočilu $m_i \in \{0,1\}^*$ kjer velja $m_i \neq m_j$ za $i \neq j$;
2. Izračunaj $\mu = \sum_{i=1}^{\ell} \mu_i$;

Agregatni podpis je μ.

Algoritem 6.4.6 Preverjanje agregatnega podpisa

Vhodni podatki: agregatni podpis μ, uporabniki $U \subseteq \mathcal{U}$, $u_i \in U, i = 1, \ldots, \ell =\mid U \mid$, sporočila $m_i \in \{0,1\}^*$.
Rezultat: veljavnost podpisa.

1. **if** $m_i = m_j, i \neq j$ **then**
   Zavrži;

2. **else**
   Izračunaj $M_i = H(m_i)$ za $1 \leq i \leq \ell =\mid U \mid$;
   if $e(\mu, P) = \prod_{i=1}^{\ell} e(M_i, a_i P)$, **then**
   Podpis je veljaven;
   else
   Podpis ni veljaven;
   end if

3. **end if**

Vsak uporabnik u_i ima privatni ključ $a_i \in [1, q-1]$ in javni ključ $a_i P$. Podpis μ_i uporabnika u_i je pravilen, če velja $\mu_i = a_i H(m_i)$. Agregatni podpis μ je torej $\mu = \sum_i \mu_i = \sum_i a_i H(m_i)$. Če uporabimo zdaj lastnosti bilinearnega parjenja, dobimo naslednje:

$$e(\mu, P) = e(\sum_i a_i H(m_i), P) = \prod_i e(H(m_i), P)^{a_i} = \prod_i e(H(m_i), a_i P).$$

Analiza varnosti tako generiranih agregatnih podpisov je opisana v [23].

6.5 Drugi primeri uporabe

V prejšnjih razdelkih smo na kratko opisali nekaj aktualnih primerov uporabe parjenj na eliptičnih krivuljah v kriptografiji. Seveda to niso edini primeri uporabe. Parjenja lahko uporabimo tudi za slepe podpise [155], prstan podpise [155, 3] ter druge digitalne podpise [3, 156]. Uporabljajo se tudi v različnih shemah, ki temeljijo na identiteti uporabnika [31, 142] in drugje. Določeni protokoli in sheme so bile tudi predlagane za vključitev v standarde [108]. Več o primerih uporabe je na voljo na [158] in v [16, 76].

Poglavje 7

PARJENJEM PRIJAZNE ELIPTIČNE KRIVULJE

V prejšnjih poglavjih smo si ogledali parjenja na eliptičnih krivuljah. Videli smo, da morajo imeti za učinkovito in varno implementacijo parjenj, eliptične krivulje posebne lastnosti. Te so majhna vključitvena stopnja k, podgrupa točk velikega praštevilskega reda r in velik razširjen obseg $\mathbb{F}_{q^k}$. Eliptičnim krivuljam, ki bodo zadoščale tem zahtevam, bomo rekli parjenjem prijazne eliptične krivulje, natančna definicija je v 7.3.1.

V tem poglavju bomo najprej predstavili dopolnjeno razvrstitev oziroma taksonomijo eliptičnih krivulj, katere osnova bo [49]. Temu bo sledila primerjava velikosti različnih parametrov, ki so bistveni za varnost. Pri tem bomo primerjali velikosti ključev za simetrične kriptosisteme, moč podgrupe na eliptični krivulje, velikost razširjenega obsega in vključitveno stopnjo. Nadaljevali bomo z eksplicitno definicijo parjenjem prijaznih eliptičnih krivulj in družin krivulj. Ker imajo vse predstavljene konstrukcije skupen osnovni princip, si ga bomo podrobneje ogledali. Pri tem bomo uporabili definicije in lastnosti eliptičnih krivulj s kompleksnim množenjem, ki smo jih pokazali v razdelku 4.9. Ko bomo imeli osnovne principe razložene, si bomo po vrsti glede na razvrstitev ogledali konstrukcije krivulj, kar je tudi glavni namen tega poglavja. Pri tem se bomo oprli na taksonomijo, ki so jo originalno predstavili Freeman, Scott in Teske leta 2010 [49] in vsebuje klasifikacijo znanih metod za generiranje eliptičnih krivulj s predpisano vkključitveno stopnjo. Dodali bomo nekaj novih algoritmov, ki so se pojavili v zadnjih letih. Predstavitev konstrukcij krivulj bomo začeli s supersingularnimi krivuljami in navadnimi krivuljami, ki niso v družinah. Temu bodo sledile konstrukcije redkih družin, polnih družin in družin z variabilno diskriminanto. Nato bomo navedli nekaj faktorjev, ki vplivajo na učinkovito in varno implementacijo, kot so distorzijske preslikave, ovoji in kompresije, aritmetika v obsegih in Hammingova utež. Poglavje bomo zaključili s seznamom priporočenih krivulj za vključitveno stopnjo $k \leq 50$.

Čeprav so si konstrukcije med seboj podobne, so vse podane z namenom, da dobimo zgoraj omenjen seznam krivulj. Seznam je povzet po [49] in dopolnjen z novimi konstrukcijami za vrednosti $k = 8, 16$ in 24.

V poglavju bomo pogosto uporabljali lastnosti ciklotomičnih polinomov. Definicije in osnovne lastnosti so podane v dodatku A.2.6. Povsod bomo uporabljali naslednje oznake:

- ζ_k označuje k-ti primitivni koren enote v $\overline{\mathbb{Q}}$;

- $\mathbb{Q}(\zeta_k)$ označuje obseg $\mathbb{Q}$ razširjen z ζ_k;
- $\Phi_k(x)$ označuje k-ti ciklotomični polinom;
- $\varphi(k)$ označuje vrednost Eulerjeve funkcije za število k.

V poglavju določenih izrekov zaradi obsežnosti in zahtevne uporabe teorije števil ne bomo dokazali. Dokazi teh so na voljo v referencah. Večino predstavljenih konstrukcij pa je podanih skupaj z dokazi.

7.1 Taksonomija

Kot smo omenili že zgoraj, si bomo najprej ogledali razvrstitev oziroma taksonomijo parjenjem prijaznih eliptičnih krivulj. Originalno taksonomijo so leta 2010 predstavili Freeman, Scott in Teske [49], naša razvrstitev, podana v diagramih 7.1, 7.2 in 7.3, se od nje poleg novih konstrukcij krivulj, razlikuje v novo dodani skupini družin krivulj z variabilno diskriminanto. Originalna taksonomija sicer vključuje tudi konstrukcije z variabilno diskriminanto, vendar so se leta 2012 pojavili novi algoritmi za take krivulje [89], zato smo to skupino dodali kot posebno v taksonomijo. Definicija posameznih družin bo podana v naslednjih razdelkih.

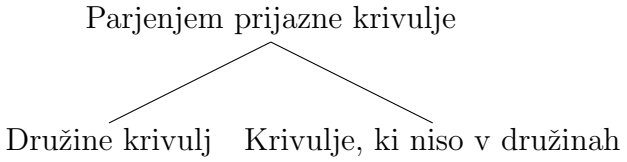


Diagram 7.1: Klasifikacija parjenjem prijaznih krivulj

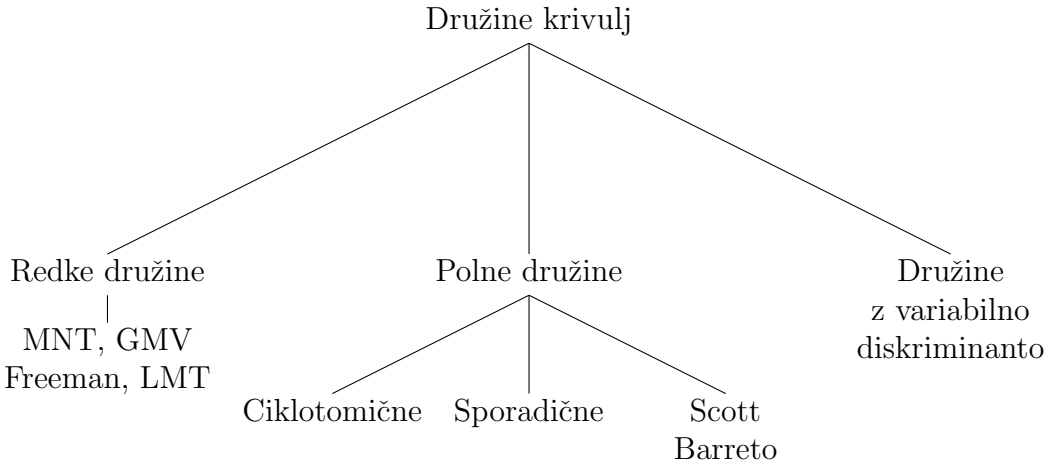


Diagram 7.2: Družine parjenjem prijaznih krivulj

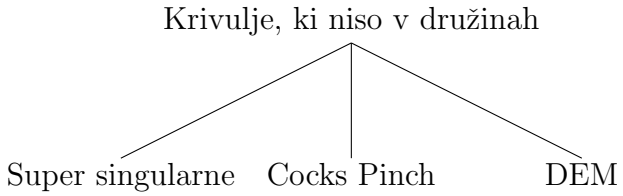


Diagram 7.3: Parjenjem prijazne krivulje, ki niso v družinah

7.2 Varnost in velikost parametrov

Preden predstavimo konstrukcije iskanih krivulj, si poglejmo, kako na varnost vplivata parametra r (velikost največje podgrupe $E(\mathbb{F}_q)$) in q^k (velikost razširitvenega obsega). Ker je računanje diskretnega logaritma v končnih obsegih bolj učinkovito kot v grupi na eliptičnih krivuljah, mora biti q^k precej večja od r. V tabeli 7.2.1 je primerjava velikosti parametrov, pri čemer smo se oprli na rezultate v [49, 56, 90], [15] in standarde [121, 122].

Iz tabele 7.2.1 vidimo, da za doseganje različnih stopenj varnosti, potrebujemo različne krivulje z različnimi vrednostmi parametrov. Za vključitveno stopnjo imamo dve različni vrednosti, ker razmerje med velikostjo razširitvenega obsega q^k in velikostjo podgrupe r ni odvisna samo od vključitvene stopnje k. Odvisna je tudi od razmerja med velikostjo osnovnega obsega q in velikostjo podgrupe r na eliptični krivulji, ki ga označimo z $\rho = \log q / \log r$. Če bi hoteli postaviti sistem, kjer bi bila velikost podgrupe 160-bitov, velikost razširitvenega obsega pa 1280-bitov, bi lahko izbrali eliptično krivuljo z vključitveno stopnjo $k = 8$ in $\rho = 1$ (take krivulje zaenkrat ne poznamo [49]), ali pa bi izbrali krivuljo z vključitveno stopnjo $k = 4$ in $\rho = 2$, oziroma vse krivulje, katerih parametri bi zadoščali enakosti $\rho \cdot k = 8$.

Splošno so zaželene krivulje, katerih vrednost ρ je majhna, saj to pospeši aritmetiko na krivulji. Tako je na primer krivulja z velikostjo podgrupe 160-bitov in $\rho = 1$ definirana nad 160-bitnim obsegom, medtem ko je krivulja s 160-bitno podgrupo in $\rho = 2$ definirana nad 320-bitnim obsegom. Po drugi strani pa je večji kvocient ρ zaželen za hitrejše računanje parjenja. Če bi pri varnostni stopnji 80 bitov vzeli 512-bitni q in 160-bitni r in vrednost $k = 2$, bi bil to za določene protokole primeren izbor parametrov [133], zato je $k = 2$, označen z *, dodan v tabeli pri stopnji varnosti 80 bitov.

7.3 Konstrukcija parjenjem prijazne eliptične krivulje

Za uporabo parjenj v kriptografiji mora biti vključitvena stopnja k krivulje E (definirana v 4.7) dovolj majhna, da je parjenje enostavno izračunljivo, vendar dovolj velika, da je diskretni logaritem v obsegu $\mathbb{F}_{q^k}^*$ težak problem. Za naključne krivulje E nad obsegom $\mathbb{F}_q$ s praštevilsko močjo podgrupe $r \approx q$ je verjetnost, da ima E vključitveno stopnjo manjšo od $\log_2 q$ glede na r majhna, in v splošnem lahko pričakujemo, da bo vključitvena stopnja v rangu velikosti parametra r [5]. Ti rezultati namigujejo, da so v primerih, ko sta r in q reda velikosti 2^{160}, rezultati parjenja na naključni krivulji v obsegu velikosti reda 2^{160}, kar pa je praktično neizvedljivo zaradi zahtevnega računanja. Da pa se izognemo Pohlig-Hellmanovem napadu [119], pa morajo imeti točke na krivulji $E(\mathbb{F}_q)$ praštevilski

Velikost ključev v sim. kriptosistemih v bitih	Velikost podgrupe r na E v bitih	Velikost razširitvenega obsega q^k v bitih	Vključitvena stopnja k glede na ρ	
			$\rho \approx 1$	$\rho \approx 2$
80	160	960 - 1340	6 - 8	2^*, 3-4
112	224	2200 - 3600	10 - 16	5 - 8
128	256	3000 - 5000	12 - 20	6 - 10
192	384	8000 - 10000	20 - 26	10 - 13
256	512	14000 - 26300	28 - 36	14 - 18

Tabela 7.2.1: Velikosti parametrov v bitih in pripadajoče vključitvene stopnje za različne stopnje varnosti

red. Naloga je torej najti krivuljo, ki ima veliko podgrupo praštevilskega reda in majhno vključitveno stopnjo. Takim krivuljam bomo rekli parjenjem prijazne krivulje, bolj natančno pa ta pojem opisuje naslednja definicija povzeta po [49].

Definicija 7.3.1. Eliptična krivulja E nad obsegom $\mathbb{F}_q$ je **parjenjem prijazna**, če sta izpolnjena naslednja pogoja:

1. Obstaja praštevilo $r \geq \sqrt{q}$, ki deli moč grupe $\#E(\mathbb{F}_q)$;
2. Vključitvena stopnja k krivulje E glede na r je manjša od $\log_2(r)/8$.

V zgornji definiciji spodnja meja za velikost podgrupe velikosti r temelji na rezultatu Luca, Shparlinski [95]. Slednji nam pove, da je krivulj z majhno vključitveno stopnjo glede na r veliko, če je $r < \sqrt{q}$ in zelo malo, če je $r > \sqrt{q}$. Zgornja meja za vključitveno stopnjo pa temelji na praktičnem interesu in zaželeni stopnji varnosti. Tako vrednost $\log_2(r)/8$ predstavlja mejo glede na vrednosti k navedenimi v tabeli 7.2.1. Če želimo spreminjati vključitveno stopnjo k, da bi dosegli višjo stopnjo varnosti, je potrebno konstruirati parjenjem prijazne krivulje. Metod za konstrukcijo takih krivulj je kar nekaj, vse pa imajo skupno naslednjo visoko-nivojsko strukturo:

1. Fiksiraj k in izračunaj taka cela števila t, r in q, za katere obstaja eliptična krivulja $E/\mathbb{F}_q$, ki ima naslednje lastnosti:
   - Sled (definirana v izreku 4.6.3) enako t;
   - Podgrupo praštevilskega reda r;
   - Vključitveno stopnjo k.
2. Uporabi metodo kompleksnega množenja za iskanje enačbe krivulje E nad obsegom $\mathbb{F}_q$ (glej razdelek 4.9.3).

Najtežji del takih metod je najti parametre v točki 1., da bo točka 2. izračunljiva. Navadna eliptična krivulja s temi lastnostmi je lahko generirana natanko tedaj, ko so izpolnjeni naslednji pogoji:

1. q je praštevilo ali potenca praštevila;
2. r je praštevilo;
3. Števili t in q sta si tuji;

4. Število r deli $q+1-t$;

5. Število r deli q^k-1 in r ne deli q^i-1 za $1 \leq i < k$;

6. Za neko dovolj majhno naravno število D in neko celo število y velja naslednja enakost:
$$4q - t^2 = Dy^2. \tag{7.1}$$

Diofantska enačba (7.1) v točki 6. izvira iz kompleksnega množenja in smo jo srečali v razdelku 4.9.3 na strani 62. Zato ji pravimo tudi **enačba kompleksnega množenja**.

Pogoj 1. zagotavlja, da obstaja končni obseg s q elementi. V večini primerov v nadaljevanju bo q praštevilo. Iz pogoja 6. sledi, da je $t \leq 2\sqrt{q}$, kar skupaj s pogojem 3. zagotovi, da obstaja navadna eliptična krivulja E definirana nad $\mathbb{F}_q$ z močjo grupe $\#E(\mathbb{F}_q) = q+1-t$ [151, izrek 4.1]. Pogoja 2. in 4. nam povesta, da ima $E(\mathbb{F}_q)$ podgrupo reda r, po trditvi 4.7.2 pa je pogoj 5. ekvivalenten temu, da je vključitvena stopnja E enaka k glede na r. Če taki parametri t, r, q obstajajo, potem obstaja navadna eliptična krivulja $E/\mathbb{F}_q$ z vključitveno stopnjo k in podgrupo reda r. Zahteva v pogoju 6., da je D dovolj majhen, je potrebna za iskanje enačbe take krivulje z metodo kompleksnega množenja, ki smo jo predstavili v razdelku 4.9. Dovolj majhno pomeni, da je $D < 10^{12}$. Ta meja nam pri računski zahtevnosti zgoraj omenjenega postopka, ki je $O(D^{1+\epsilon})$ za nek $\epsilon \in \mathbb{R}_{>0}$ [143], omogoča izračun enačbe krivulje v realnem času. Če uporabimo pogoj 4. in zapišemo $q+1-t = hr$ za nek h, potem enačbo (7.1) lahko zapišemo v obliki
$$Dy^2 = 4hr - (t-2)^2. \tag{7.2}$$

Vrednosti h v zgornji enačbi pravimo tudi **kofaktor** parjenjem prijazne krivulje.

Naslednja trditev bo ključna pri konstrukciji krivulj.

Trditev 7.3.2. *Naj bo k naravno število, r praštevilo, $E/\mathbb{F}_q$ eliptična krivulja z močjo grupe enake hr, t sled $E/\mathbb{F}_q$ in $r \nmid kq$. Potem ima krivulja $E/\mathbb{F}_q$ vključitveno stopnjo k glede na r natanko tedaj, ko je $\Phi_k(q) \equiv 0 \pmod{r}$, oziroma natanko tedaj, ko je $\Phi_k(t-1) \equiv 0 \pmod{r}$.*

Dokaz. Predpostavimo, da ima E vključitveno stopnjo k glede na r. Potem po trditvi 4.7.2 $r \mid q^k-1$ in $r \nmid q^i-1$, za $1 \leq i < k$. Če upoštevamo lastnost ciklotomičnih polinomov $x^k - 1 = \prod_{d|k} \Phi_d(x)$ in dejstvo, da je r praštevilo, sledi da $r \mid \Phi_k(q)$. Ker je $q+1-t = hr$ in $q \equiv t-1 \pmod{r}$, sledi $r \mid \Phi_k(t-1)$.

Dokažimo še obrat. Če $r \mid \Phi_k(t-1)$ potem $r \mid \Phi_k(q)$ in posledično $r \mid q^k-1$. To pomeni, da ima $E/\mathbb{F}_q$ vključitveno stopnjo kvečjemu k. Pokazati moramo še, da $r \nmid q^i - 1$ za $1 \leq i < k$. Pri temo bomo sledilu dokazu iz [100]. Naj bo $f(x) = x^k - 1$ in naj bo $\mathbb{F} = \mathbb{Z}/r\mathbb{Z}$. Ker $r \nmid k$, je $\gcd(f(x), f'(x)) = 1$ v $\mathbb{F}[x]$. Torej ima polinom $f(x)$ eno samo ničlo v $\mathbb{F}$. Zopet upoštevamo lastnost ciklotomičnih polinomov $x^k - 1 = \prod_{d|k} \Phi_d(x)$ in dejstvo, da je q koren polinoma $\Phi_k(x)$ nad $\mathbb{F}$. Tako dobimo $\Phi_d(q) \not\equiv 0 \pmod{r}$ za vsak $d \mid k$ in $1 \leq d < k$. Posledično $r \nmid q^d - 1$ za vsak $d|k$ in $1 \leq d < k$. Sledi še, da $r \nmid q^i - 1$ za vsak naravno število $i \nmid k$, saj bi v nasprotnem primeru $r \mid q^{\gcd(i,k)} - 1$. ■

Trditev 7.3.2 nam pove, da lahko pogoj 5. zgoraj zamenjamo s pogojem

5.* r deli $\Phi_k(t-1)$.

Do sedaj smo si ogledali, kako kreirati krivuljo za dane parametre q, r in t. Za uporabo v praksi pa bi radi generirali tudi krivulje določenih velikost v bitih. Za ta namen bomo opisali družine parjenjem prijaznih krivulj, za katere so parametri q, r in t dani kot polinomi $q(x)$, $r(x)$ in $t(x)$. Ideja o parametrizaciji krivulj s polinomi je bila uporabljena v različnih konstrukcijah s strani različnih avtorjev [9, 25, 107]. Definicija, ki jo bomo povzeli po [49], formalizira vse te pristope implicitno in nam predstavlja ogrodje za nadaljnje konstrukcije krivulj.

Ker bodo vrednosti polinomov $q(x)$ in $r(x)$ predstavljale velikosti obsegov in grup, morajo imeti polinomi, ki jih bomo konstruirali, lastnost, da za veliko vrednosti x zavzamejo določene vrednosti. Tako morajo biti vrednosti polinoma $q(x)$ potence praštevila, vrednosti polinoma $r(x)$ pa praštevilo ali pa produkt praštevila in kofaktorja.

O praštevilskih vrednostih polinomov je znanega malo [99]. Tako na primer ni znano niti za polinom, kot je na primer $x^2 - 1$, koliko praštevilskih vrednosti zavzame, oziroma ali je le teh neskončno. Zato moramo zahtevati izpolnjevanje dodatnih pogojev, če želimo, da polinomi, ki jih bomo v nadaljevanju konstruirali, zavzamejo praštevilske vrednosti.

Definicija 7.3.3. Naj bo $f(x)$ polinom z racionalnimi koeficienti. Pravimo da f **predstavlja praštevila**, če so izpolnjeni naslednji pogoji:

1. $f(x)$ je nekonstanten polinom;
2. $f(x)$ ima pozitivni vodilni koeficient;
3. $f(x)$ je nerazcepen;
4. $f(x) \in \mathbb{Z}$ za nekaj vrednosti $x \in \mathbb{Z}$ (ekvivalentno, za neskončno mnogo $x \in \mathbb{Z}$);
5. $\gcd(\{f(x) : x, f(x) \in \mathbb{Z}\}) = 1$.

Opomba: Zgornja definicija je povzeta po [49] in je motivirana z znano hipotezo Buniakowskega in Schnizela [85], ki pravi, da nekonstanten polinom $f(x) \in \mathbb{Z}[x]$ zavzame neskončno mnogo praštevilskih vrednosti natanko tedaj, ko ima pozitivni vodilni koeficient, ko je nerazcepen in ko velja $\gcd(\{f(x) : x \in \mathbb{Z}\}) = 1$. Hipoteza Batemana in Horna [12] generalizira ta rezultat tudi na polinome z racionalnimi koeficienti. To hipotezo bomo pri konstrukcijah v nadaljevanju uporabili pri dokazovanju, da polinomi predstavlja praštevila.

Vsak pogoj v definiciji 7.3.3 je potreben za to, da f zavzame neskončno mnogo praštevilskih vrednosti, zadostnost pogojev pa je hipotetična. Testiranje, ali polinom $f(x)$ predstavlja praštevilo, je izvedeno s končnim postopkom:

- Pogoj 4. testiramo tako, da izračunamo vrednosti $f(x)$ za vsa cela števila $x \in [0, N)$ za nek tak N, da je $N \cdot f(x) \in \mathbb{Z}$;
- Pogoj 5. testiramo tako, da za $n \in \mathbb{Z}$ izračunamo $f(n) \in \mathbb{Z}$ in preverimo, ali je $f(x)$ enaka 0 po $\mod p$ za vsa praštevila p, ki delijo $f(n)$.

Dodatno, če je $f(x) = \pm 1$ za nek x ali če $f(x)$ zavzame dve različni praštevilski vrednosti, potem sta oba pogoja 4. in 5. izpolnjena.

Preden dokončno definiramo družine parjenjem prijaznih eliptičnih krivulj po [49], potrebujemo še nekaj dodatnih orodij.

Definicija 7.3.4. Polinom $f(x) \in \mathbb{Q}[x]$ ima **celoštevilske vrednosti**, če $f(x) \in \mathbb{Z}$ za vsak $x \in \mathbb{Z}$.

Primer. Polinom $f(x) = \frac{1}{2}(x^2 + x + 2) = \frac{x(x+1)}{2} + 1$ ima celoštevilske vrednosti in predstavlja praštevila. •

Definicija 7.3.5. Naj bodo $t(x)$, $r(x)$ in $q(x)$ neničelni polinomi z racionalnimi koeficienti.

1. Za dano naravno število k in naravno število D prosto kvadratov, trojka (t, r, q) **parametrizira družino eliptičnih krivulj z vključitveno stopnjo k in diskriminanto D**, če so izpolnjeni naslednji pogoji:
   (a) $q(x) = p(x)^d$ za nek $d \in \mathbb{N},\ d \geq 1$ in polinom $p(x)$, ki predstavlja praštevilo;
   (b) $r(x)$ je nekonstanten, nerazcepen, ima celoštevilske vrednosti in pozitivni vodilni koeficient;
   (c) $r(x)$ deli polinom $q(x) + 1 - t(x)$;
   (d) $r(x)$ deli polinom $\Phi_k(t(x) - 1)$, kjer je Φ_k k-ti ciklotomični polinom;
   (e) enačba
   $$Dy^2 = 4q(x) - t(x)^2 \tag{7.3}$$
   ima neskončno celoštevilskihh rešitev (x, y).

   Če so ti pogoji izpolnjeni, trojko (t, r, q) imenujemo **družina**.
2. Naj bo trojka (t, r, q) družina. Če je x_0 celo število in E eliptična krivulja nad obsegom $\mathbb{F}_{q(x_0)}$ s sledjo $t(x_0)$, potem pravimo, da je E **krivulja družine** (t, r, q)**.**
3. Družina (t, r, q) je **navadna** (ang. ordinary), če je $\gcd(t(x), q(x)) = 1$.
4. Družina (t, r, q) je **polna** (ang. complete), če obstaja tak polinom $y(x) \in \mathbb{Q}[x]$, da velja $Dy(x)^2 = 4q(x) - t(x)^2$.
5. Družina (t, r, q) je **polna z variabilno diskriminanto**, če se enačba v (7.3) da zapisati bodisi kot
   $$f(x)y(x)^2 = 4q(x) - t(x)^2, \tag{7.4}$$
   bodisi kot
   $$f(x) = 4q(x) - t(x)^2, \tag{7.5}$$
   kjer je $f(x)$ linearni polinom.
6. Če družina ne zadošča nobenemu od pogojev v točkah 3., 4. in 5. je družina **redka** (ang. sparse).
7. Trojka (t, r, q) parametrizira **potencialno** družino krivulj, če so izpolnjeni pogoji (b) - (e) točke 1. V tem primeru polinom $p(x)$ lahko predstavlja praštevilo, ali pa tudi ne.

Pogoj (c) v točki 1. definicije 7.3.5 zagotavlja, da za dano vrednost x, za katero je $q(x)$ praštevilo, število $r(x)$ deli moč grupe $\#E(\mathbb{F}_{q(x)})$. Če je $r(x) = q(x)+1-t(x)$, potem je za vrednosti x, za katere sta $r(x)$ in $q(x)$ praštevili tudi $\#E(\mathbb{F}_{q(x)})$ praštevilo. To je idealni primer, ki pa ga je v praksi težko doseči. Zato definiramo parameter ρ, ki nam pove, kako blizu tega idealnega primera je dana krivulja družine. Parameter ρ izraža razmerje med velikostjo q obsega in velikostjo r podgrupe $E(\mathbb{F}_q)$ praštevilskega reda.

Definicija 7.3.6.

1. Naj bo $E/\mathbb{F}_q$ eliptična krivulja, ki ima podgrupo reda r. **Vrednost ρ krivulje** E glede na r je definirana kot
$$\rho(E) = \frac{\log q}{\log r}. \tag{7.6}$$

2. Naj trojka (t, r, q) parametrizira družino (oziroma potencialno družino) eliptičnih krivulj z vključitveno stopnjo k. **Vrednost ρ družine** (t, r, q) je definirana kot
$$\rho(t, r, q) = \lim_{x\to\infty} \frac{\log q(x)}{\log r(x)} = \frac{\deg(q)}{\deg(r)}. \tag{7.7}$$

Po definiciji 7.3.1 imajo parjenjem prijazne krivulje $\rho(E) \leq 2$. Po drugi strani pa iz Hassejeve meje $|\#E(\mathbb{F}_q) - q + 1| \leq 2\sqrt{q}$ sledi, da je vrednost $\rho(t, r, q)$ vedno vsaj 1. Če obstajajo krivulje v družini (t, r, q), katerih red je praštevilo, potem $\deg(r) = \deg(q)$ in $\rho(t, r, q) = 1$. To je idealni primer, vendar pa obratno ni nujno res. Če je $\rho(t, r, q) = 1$, je lahko za vsako krivuljo E v tej družini $\#E(\mathbb{F}_q) = hr(x)$, kjer je h konstanten kofaktor [56]. V trditvi 7.3.7 je nekaj lastnosti vrednosti ρ za navadne eliptične krivulje s stopnjo vključitve 1 ali 2.

Trditev 7.3.7. *Naj bo trojka (t, r, q) družina navadnih eliptičnih krivulj s stopnjo vključitve $k \leq 2$ in diskriminanto D. Potem velja:*

1. *Če je $k = 1$, potem je $\rho(t, r, q) \geq 2$, kadar velja katerikoli od naslednjih pogojev:*
   (a) $\deg(t) \geq 1$;
   (b) *Obstaja neskončno mnogo celoštevilskih rešitev (x, y) enačbe kompleksnega množenja* (7.3)*, za katere je vrednost polinoma $r(x)$ prosta kvadratov in tuja k D.*

2. *Za $k = 2$ je $\rho(t, r, q) \geq 2$.*

Dokaz. Iz pogoja (c) v točki 1. definicije družine 7.3.5 sledi $r(x) \mid \Phi_k(t(x) - 1)$. Po definiciji ciklotomičnega polinoma A.2.42 je za $1 \leq k \leq 2$ $\deg(\Phi_k) = 1$ in v primeru, ko je $\Phi_k(t(x) - 1) \neq 0$ je $\deg(t) \geq \deg(r)$. Iz Hassejeve meje potem sledi $\rho(t, r, q) \geq 2$. Ostaneta še primera $k = 1$, $t(x) = 2$ in $k = 2$, $t(x) = 0$. Če je $t(x) = 0$, potem družina ni navadna, zato drugi primer lahko zavržemo. Če pa je $k = 1$ in $t(x) = 2$, potem enačba kompleksnega množenja (7.2) dobi obliko $Dy^2 = 4h(x)r(x)$. Iz predpostavke (b) točke 1. trditve sledi, da je neskončno mnogo vrednosti x, za katere je $h(x) \geq r(x)$ in posledično je $\deg(h) \geq \deg(r)$. Ker je $\deg(q) = \deg(h) + \deg(r)$, sledi $\rho(t, r, q) \geq 2$. ■

7.4 Supersingularne krivulje

Spomnimo se, da je eliptična krivulja $E/\mathbb{F}_q$ z grupo točk moči $\#E(\mathbb{F}_q) = q + 1 - t$ supersingularna natanko tedaj, ko je $\gcd(t, q) > 1$ (glej definicijo 4.8.3). Dokazano je, da so redi grup supersingularnih krivulj oblike $q + 1 - t$, kjer je $t^2 \in \{0, q, 2q, 3q, 4q\}$ [136]. Iz tega sledi, da imajo suersingularne krivulje vključitveno stopnjo $k \in \{1, 2, 3, 4, 6\}$, kar

smo dokazali v izreku 4.8.5. Velja še več, $k = 2$ je edina možna vrednost za krivulje nad praštevilskimi obsegi $\mathbb{F}_q$ za $q \geq 5$, kar smo dokazali v posledici 4.8.7.

Edina znana metoda za kreiranje supersingularne krivulje je redukcija krivulj s kompleksnim množenjem v karakterisitiki 0 [27]. Natančneje, krivulji s kompleksnim množenjem $y^2 = x^3 + ax$ in $y^2 = x^3 + b$ definirani nad $\mathbb{Q}$ se reducirata v supersingularne krivulje nad $\mathbb{F}_p$ za vsa liha praštevila $p \equiv 3 \pmod 4$ in $p \equiv 2 \pmod 3$ zaporedoma. Za večino aplikacij ti dve krivulji zadoščata, konstrukcijo supersingularne krivulje nad poljubnim praštevilskim obsegom pa si bomo ogledali v algoritmu 7.4.1.

Ker supersingularna krivulja z vključitveno stopnjo $k \neq 2$ ne more biti definirana nad praštevilskim obsegom, bomo v tem razdelku upoštevali tudi ne-praštevilske obsege, kjer pa se bomo zaradi učinkovitosti omejili zgolj na tiste s karakteristiko 2 ali 3 in na obsege oblike $\mathbb{F}_{p^2}$ za velika praštevila p. Supersingularne krivulje so zaradi MOV in Frey-Rück napadov na ECDLP [101, 51], kar smo opisali v 6.1, dolgo veljale kot krivulje neprimerne za uporabo v kriptografiji. V shemah s parjenjem pa imajo zaradi svojih lastnosti določene prednosti.

7.4.1 Vključitvena stopnja $k = 1$

Supersingularne krivulje z vključitveno stopnjo $k = 1$ obstajajo samo nad končnim obsegom $\mathbb{F}_q$, kjer je $q = p^s$, p praštevilo in $s \in \mathbb{N}$ liho [101]. V tem primeru mora biti $t = \pm 2\sqrt{q}$ in posledično $\#E(\mathbb{F}_q) = q \pm 2\sqrt{q} + 1$ (glej izrek 4.8.6). Ker red podgrupe deli $\#E(\mathbb{F}_q)$ in $\Phi_k(1) = q - 1$, mora biti r faktor števila $\gcd(\#E(\mathbb{F}_q), q - 1) = \sqrt{q} \pm 1$. Posledično imajo take krivulje vrednost $\rho = \log q / \log r \geq 2$.

Za konstrukcijo take krivulje, naj bo $q' = \sqrt{q}$ in naj bo $E/\mathbb{F}_{q'}$ krivulja, katere Frobeniusova sled $t = 0$, tj. $\#E(\mathbb{F}_{q'}) = q' + 1$. Karakteristični polinom q'-te potence Frobeniusovega endomorfizma, definiran v definiciji 4.6.7, je enak $x^2 + q'$ in se razcepi v faktorja $(x + i\sqrt{q'})(x - i\sqrt{q'})$, kjer je $i = \sqrt{-1}$. Weilova domneva [137, izrek V.2.2] nam pove, da je karakteristični polinom q-te potence Frobeniuseovega endomorfizma $(x + q')^2$. Posledično velja $\#E(\mathbb{F}_q) = (q' + 1)^2 = q + 2\sqrt{q} + 1$. Kljub temu, da ima $E/\mathbb{F}_{q'}$ vključitveno stopnjo enako 2, ima krivulja E, če jo gledamo nad obsegom $\mathbb{F}_q$, vključitveno stopnjo enako 1 (glede na r). Kako se konstruira krivulja nad $\mathbb{F}_{q'}$ s sledjo enako 0 in podgrupo reda r za poljuben r, bomo videli v naslednjem podrazdelku. Ker lahko za take krivulje z izbiro reda grupe r dobimo vrednost $\log q' / \log r$ poljubno blizu 1, je lahko tudi vrednost ρ za $E/\mathbb{F}_q$ z vključitveno stopnjo 1 blizu 2. Zaključimo, da v primeru, ko želimo supersingularno krivuljo $E/\mathbb{F}_q$ s $k = 1$ in $\rho(E) = \rho_0$, lahko dobimo ekvivalentno z izbiro supersingularne krivulje $E'/\mathbb{F}_{\sqrt{q}}$ s $k = 2$ in $\rho(E') = \rho_0/2$.

7.4.2 Vključitvena stopnja $k = 2$

Primer s $k = 2$ nam nudi največ fleksibilnosti, saj lahko konstruiramo krivulje nad praštevilskim obsegom s poljubno podgrupo reda r in vrednostjo ρ. Za vključitveno stopnjo $k = 2$ je potreben pogoj $r \mid q + 1$, kar zagotovo velja, če je $t = 0$ in so lahko take krivulje definirane nad praštevilskimi in ne-praštevilskimi obsegi. V primeru, ko je karakteristika obsega 2 ali 3, obstaja same ena supersingularna krivulja do $\overline{\mathbb{F}}_q$-izomorfizma in sicer je to krivulja z j-invarianto , definirano v definiciji 4.1.1, enako nič [137, poglavje 5.4]. Nad obsegom $\mathbb{F}_q$ karakteristike 2 so krivulje s sledjo $t = 0$ dane z naslednjima enačbama

in pripadajočimi pogoji [102]:

$$\begin{aligned} E/\mathbb{F}_q: &\quad y^2+y=x^3+\delta x, && \text{če je } q=2^s \text{ za } s\in\mathbb{N} \text{ sodo in } \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_4}(\delta)\neq 0,\\ E/\mathbb{F}_q: &\quad y^2+y=x^3, && \text{če je } q=2^s \text{ za } s\in\mathbb{N} \text{ liho.}\end{aligned}$$

Konstrukcijo supersingularnih krivulj nad praštevilskimi obsegi s karakteristiko večjo od 3 pa omogoča naslednji izrek.

Izrek 7.4.1. *[84, Izrek 13.12]. Naj bo L številski obseg in E/L eliptična krivulja s kompleksnim množenjem. Naj bo $\mathrm{End}_L(E)\otimes\mathbb{Q}\cong\mathbb{Q}(\sqrt{-D})$ in naj bo $p'\,|\,p$ praštevilo v L, kjer ima E dobro redukcijo, tj. p' ne deli diskriminante krivulje Δ definirane v 4.1.1. Potem je redukcija krivulje $E \mod p'$ supersingularna natanko tedaj, ko je število p' nerazcepno v $\mathbb{Q}(\sqrt{-D})$, tj. $\left(\frac{-D}{p}\right)\neq 1$ (glej (4.13)).* ■

Če pri dani podgrupi velikosti r izberemo tak h, da je $q=hr-1$ praštevilo, potem imamo na podlagi konstrukcije Koblitza in Menezesa [81] ter Brökera [26] naslednji algoritem 7.4.1 za konstrukcijo krivulje nad obsegom $\mathbb{F}_q$ z vključitveno stopnjo $k=2$ glede na r.

Algoritem 7.4.1 Algoritem za konstrukcijo supersingularne krivulje

Vhodni podatki: praštevilo $q\geq 5$;
Rezultat: supersingularna kriuvlja $E/\mathbb{F}_q$;

1. Če $q\equiv 3 \pmod 4$, **vrni** $y^2=x^3+ax$ za poljuben $a\in{\mathbb{F}_q}^*$, $-a\notin({\mathbb{F}_q}^*)^2$;
2. Če $q\equiv 5 \pmod 6$, **vrni** $y^2=x^3+b$ za poljuben $b\in{\mathbb{F}_q}^*$;
3. Če $q\equiv 1 \pmod{12}$ naredi naslednje:
   (a) Naj bo D najmanjše tako praštevilo, da velja $D\equiv 3 \pmod 4$ in $(\frac{-D}{q})=-1$;
   (b) Izračunaj Hilbertovo razredni polinom $H_D(x)$ obsega $\mathbb{Q}(\sqrt{-D})$;
   (c) Izračunaj ničlo $j\in\mathbb{F}_q$ polinoma $H_D(x) \pmod q$;
   (d) Naj bo $m=j/(1728-j)$, **vrni** $y^2=x^3+3mc^2x+2mc^3$ za poljuben $c\in{\mathbb{F}_q}^*$.

Pričakovan čas algoritma je $\mathcal{O}((\log p)^{3+\epsilon})$ za poljuben $\epsilon>0$ [26]. Definicija Hilbertovih polinomov je v A.2.36, uporaba pa je opisana tudi v 4.9.3. Zahteva v koraku 1., da je $-a$ prost kvadratov v ${\mathbb{F}_q}^*$, garantira $E[2]\not\subset E(\mathbb{F}_q)$ in posledično ima E vključitveno stopnjo 2 glede na podgrupo reda 2 [101]. Pogoj $D\equiv 3 \pmod 4$ v točki (a) koraka 3. zagotavlja, da ima Hilbertov razredni polinom $H_D(x)$ koren v $\mathbb{F}_q$ [26]. Taka konstrukcija nam omogoča, da r in h izberemo skoraj poljubno. Za r tako lahko izberemo veliko sestavljeno število, kot na primer RSA modul [20]. Če fiksiramo poljuben $\rho_0\geq 1$ in izberemo $h\approx r^{\rho_0-1}$, lahko zagotovimo, da ima konstruirana krivulja vrednost ρ zelo blizu ρ_0. Krivulji $y^2=x^3+ax$ in $y^2=x^3+b$ iz izreka 7.4.1 sta posebna primera splošne metode, ki imata dodatno lastnost, da so distorzije definirane v 5.5.1 na njih lahko izračunljive [81].

7.4.3 Vključitvena stopnja $k = 3$

Supersingularna krivulja nad $\mathbb{F}_q$ ima vključitveno stopnjo $k = 3$ glede na podgrupo praštevilskega reda $r > 3$ natanko tedaj, ko je $q = p^s$, kjer je s sodo število in $t = \pm\sqrt{q}$ (izrek 4.8.5). Pri karakteristiki $p > 3$ ima edina taka krivulja naslednjo obliko

$$E/\mathbb{F}_q : \ y^2 = x^3 + \gamma,$$

kjer je γ nekubični element obsega ${\mathbb{F}_q}^*$ [107].

Če se omejimo na poseben primer, kjer sta $q = p^2$ in $p \equiv 2 \pmod 3$ veliko praštevilo, potem je $\#E(\mathbb{F}_{p^2}) = p^2 \pm p + 1$. Če je predznak pri drugem členu pozitiven (tj. $t = -p$), potem za $p = 3x - 1$ lahko najdemo krivuljo s praštevilskim redom, saj $r(x) = (3x - 1)^2 + (3x - 1) + 1$ predstavlja praštevilo v smislu definicije 7.3.3. Če pa je $t = p$, pa mora biti $\#E(\mathbb{F}_{p^2})$ večkratnik števila 3. Če obe ugotovitvi združimo v jeziku družin v smislu definicije 7.3.5, dobimo naslednji trojki polinomov:

$$\begin{array}{rrr} t(x) = -3x + 1, & r(x) = 9x^2 - 3x + 1, & q(x) = (3x - 1)^2; \\ t(x) = 3x - 1, & r(x) = 9x^2 - 9x + 3, & q(x) = (3x - 1)^2. \end{array} \tag{7.8}$$

Ker je $4q(x) - t(x)^2 = 3(3x - 1)^2$, trojki (t, r, q) parametrizirata družino krivulj z vključitveno stopnjo $k = 3$ in diskriminanto 3 Vrednost $\rho(t, r, q)$ te družine je 1. Če sta $r(x_0)$ in $3x_0 - 1$ praštevili za nek $x_0 \in \mathbb{Z}$, potem lahko konstruiramo krivuljo nad $\mathbb{F}_{q(x_0)}$ z vključitveno stopnjo $k = 3$ in praštevilskim redom.

Če pa je $q = 2^s$, potem imajo krivulje z vključitveno stopnjo 3 naslednjo obliko:

$$E/\mathbb{F}_q : \ y^2 + \gamma^j y = x^3 + \alpha,$$

kjer $j \in \{1, 2\}$, γ je nekubični element v ${\mathbb{F}_q}^*$ in α je ali enak 0 ali pa $\alpha \in \mathbb{F}_q$ za katerega velja $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(\gamma^{-2j}\alpha) = 1$. Če je $\alpha = 0$, je $t = \sqrt{q}$ natanko tedaj, ko $4 \nmid s$, sicer je $t = -\sqrt{q}$. Če pa je $\alpha \neq 0$, velja $t = \sqrt{q}$ natanko tedaj, ko $4 \mid s$, sicer je $t = -\sqrt{q}$ [102].

7.4.4 Vključitvena stopnja $k = 4$

Supersingularne krivulje, ki imajo vključitveno stopnjo $k = 4$ glede na podgrupo praštevilskega reda $r > 2$, obstajajo samo nad končnimi obsegi karakteristike 2 (izrek 4.8.5), posledično sta pogoja $q = 2^s$, kjer je s liho število in $t = \pm\sqrt{2q}$ potrebna [107]. Edini taki krivulji sta oblike [102]:

$$\begin{array}{ll} E/\mathbb{F}_q : & y^2 + y = x^3 + x, \\ E/\mathbb{F}_q : & y^2 + y = x^3 + x + 1. \end{array}$$

Pri prvi krivulji je $t = \sqrt{2q}$ natanko tedaj, ko je $s \equiv \pm 3 \pmod 8$, sicer je $t = -\sqrt{2q}$. Pri drugi krivulji pa je $t = \sqrt{2q}$ natanko tedaj, ko je $s \equiv \pm 1 \pmod 8$, sicer je $t = -\sqrt{2q}$ [14].

7.4.5 Vključitvena stopnja $k = 6$

Supersingularne krivulje, ki imajo vključitveno stopnjo $k = 6$ glede na podgrupo praštevilskega reda $r > 3$, obstajajo samo nad končnimi obsegi karakteristike 3 (izrek 4.8.5),

posledično sta pogoja $q = 3^s$, kjer je $s > 1$ in $t = \pm\sqrt{3q}$ potrebna [107]. Edini taki krivulji imata obliko [109]:

$$E/\mathbb{F}_q : \quad y^2 = x^3 - x + \delta \quad \text{in}$$
$$E/\mathbb{F}_q : \quad y^2 = x^3 - x - \delta,$$

kjer je $\delta \in \mathbb{F}_q$, $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_3}(\delta) = 1$ (npr. $\delta = 1$, če $s \equiv 1 \pmod 3$). Pri prvi krivulji je $t = \sqrt{3q}$ natanko tedaj, ko $4 \nmid s - 1$, sicer je $t = -\sqrt{3q}$. Pri drugi krivulji pa je $t = \sqrt{3q}$ natanko tedaj, ko $4 \mid s - 1$, sicer je $t = -\sqrt{3q}$ [14].

7.5 Navadne krivulje s poljubno vključitveno stopnjo

V tem razdelku si bomo najprej ogledali najbolj znani metodi v literaturi in sicer Cocks-Pinch metodo [34] in Dupont-Enge-Morain metodo [42]. Metodi lahko uporabimo za konstrukcijo parjenjem prijaznih krivulj, vendar obe generirata krivulje z vrednostjo $\rho \approx 2$, ki morda niso primerne za določene aplikacije. Nobena metoda ne generira družin krivulj v smislu definicije 7.3.5, vendar posplošitev Cocks-Pinch metode, ki si jo bomo ogledali kasneje v razdelku 7.7.1, lahko generira družino krivulj z vrednostjo $\rho < 2$. Poleg tega Cocks-Pinch metoda lahko generira krivulje s praštevilskim redom podgrupe poljubne velikosti. Podgrupe krivulj generiranih z Dupont-Enge-Morain metodo pa morajo imeti red r, ki je vrednost določenega polinoma in je zato le-ta težje določljiva.

7.5.1 Cocks-Pinch metoda

Cocks-Pinch metoda generira krivuljo tako, da najprej fiksira podgrupo velikosti r in diskriminanto kompleksnega množenja D, ter nato izračuna tako sled t in praštevilo q, da je zadoščeno enačbi kompleksnega množenje (7.1).

Izrek 7.5.1. *[34]. Fiksirajmo $k \in \mathbb{N}$ in naj bo D naravno število prosto kvadratov.*

1. *Naj bo r tako praštevilo, da $k \mid r - 1$ in $\left(\frac{-D}{r}\right) = 1$.*
2. *Naj bo ζ k-ti koren enote v $(\mathbb{Z}/r\mathbb{Z})^*$ (tak ζ obstaja, ker $k \mid r - 1$) in $t' = \zeta + 1$.*
3. *Naj bo $y' = (t' - 2)/\sqrt{-D} \pmod r$.*
4. *Naj bo $t \in \mathbb{Z}$ kongruenten $t' \pmod r$ in naj bo $y \in \mathbb{Z}$ kongruenten $y' \pmod r$. Naj bo $q = (t^2 + Dy^2)/4$.*

Če je q praštevilo, potem obstaja eliptična krivulja E nad obsegom $\mathbb{F}_q$ s podgrupo točk reda r in vključitveno stopnjo k. Če je $D < 10^{12}$ se E lahko konstruira z metodo kompleksnega množenja. ■

Ključni del algoritma oziroma izreka 7.5.1 je v tem, da je y konstruiran tako, da $r \mid Dy^2 + (t-2)^2$. S tako izbiro praštevila q, da je zadoščeno enačbi kompleksnega množenje $4q - t2 = Dy^2$, dobimo $4(q + 1 - t) \equiv 0 \pmod r$. Izbira vrednosti t pa zagotavlja, da je $\Phi_k(t - 1) \equiv 0 \pmod r$.

Opomba: Za števili t in y ni razloga, da bi bili precej manjši od števila r, zato lahko sklepamo, da je v večini primerov $q \approx r^2$. Posledično sklepamo, da ima večina krivulj

generiranih s to metodo vrednost $\rho \approx 2$. V koraku 4. izreka 7.5.1 lahko števili t in y izberemo kot poljubni celi števili kongruentni t' in q' $(\mathrm{mod}\ r)$ zaporedoma. Tako lahko, če želimo generirati krivuljo z dano vrednostjo $\rho_0 \geq 2$, vrednostim t in y prištejemo naravno število deljivo z r velikosti približno $r^{\rho_0/2}$. Cocks-Pinch metoda se lahko uporabi pri konstrukciji eliptične krivulje z vključitveno stopnjo k glede na r tudi v primeru, ko je r veliko sestavljeno število (RSA parameter) [22].

7.5.2 Dupont-Enge-Morain metoda

Cocks-Pinch metoda fiksira r in potem izračuna števili t in q, da je zadoščeno enačbi kompleksnega množenja 7.1. Pristop Dupont, Enge, Morain [42] pa je drugačen in sicer metoda izračuna števili t in r hkrati, z uporabo rezultant (definiranih v dodatku A.3).

Izrek 7.5.2. *[42]. Fiksirajmo $k \in \mathbb{N}$.*

1. *Naj bo*
$$R(a) = R(\Phi_k(x-1), a + (x+2)^2) \in \mathbb{Z}[a]$$
rezultanta.

2. *Naj bo $a \in \mathbb{Z}$ tak, da je $R(a)$ praštevilo in naj bo $r = R(a)$.*

3. *Naj bo $g(x) = \gcd(\Phi_k(x-1), a + (x-2)^2) \in \mathbb{F}_r[x]$ in naj bo $t' \in \mathbb{F}_r$ koren polinoma g.*

4. *Naj bo $t \in \mathbb{Z}$ kongruentno t' $(\mathrm{mod}\ r)$ in naj bo $q = (t^2 + a)/4$.*

Če je q praštevilo, potem obstaja eliptična krivulja nad $\mathbb{F}_q$ s podgrupo točk reda r in vključitveno stopnjo k. Če je $a = Dy^2$ in $D < 10^{12}$, potem se E lahko konstruira z metodo kompleksnega množenja. ■

Ključna ideja Dupont-Enge-Morain metode je v naslednji lastnosti rezultante: če sta $f(x)$ in $g(x)$ polinoma nad obsegom K, potem je $R(f(x), g(x)) = 0$ natanko tedaj, ko imata $f(x)$ in $g(x)$ skupno ničlo v $\overline{K}$ [85, posledica IV.8.4]. Če gledamo $\Phi_k(x-1)$ in $a + (x-2)^2$ kot polinoma v dveh spremenljivkah a in x, je rezultanta R polinom ene spremenljivke a stopnje $\varphi(k)$. Če a izberemo tak, da je $r = R(a)$ praštevilo, potem je $R(a) \equiv 0 \pmod{r}$ in posledično imata $\Phi_k(x-1)$ in $a + (x-2)^2$ skupen faktor $g(x)$, če ju gledamo kot polinoma po $\mathrm{mod}\ r$, tj. v $\mathbb{F}_r[x]$. V lemi 7.5.3 bomo dokazali, da je $r \equiv 1 \pmod{k}$, iz česar sledi, da $\Phi_k(x)$ razpade v dva linearna faktorja v $\mathbb{F}_r[x]$. Ker $g(x) \mid \Phi_k(x)$, ima polinom $g(x)$ koren $t' \in \mathbb{F}_r$. Tako izračunani vrednosti t in r zadoščata pogojema $t \mid \Phi_k(x-1)$ in $r \mid Dy^2 + (t-2)^2$. S q konstruiranim v točki 4. izreka 7.5.2 je enačba kompleksnega množenja rešljiva in posledično velja $q + 1 - t \equiv 0 \pmod{r}$.

Opomba: Podobno kot pri Cocks-Pinch metodi, tudi tu velja, da t ni precej manjši od r in v splošnem $q \approx r^2$. Posledično lahko sklepamo, da ima večina krivulj generiranih s to metodo vrednost ρ blizu 2.

Naslednja lema, katere dokaz je na voljo v [49], potrdi domnevo, da ni težko najti takih vrednosti za a, da je $R(a)$ v točki 2. izreka 7.5.2 praštevilo.

Lema 7.5.3. *[49, Lema 4.5]. Fiksirajmo naravno število k in naj bo $R(a) \in \mathbb{Z}[a]$ definirana kot v točki 1. izreka 7.5.2. Potem $R(a)$ predstavlja praštevilo glede na definicijo 7.3.3. V posebnem velja $R(a) \equiv 1 \pmod{k}$, če je $R(a)$ liho praštevilo za nek $a \in \mathbb{Z}$.* ■

Podobno kot Cocks-Pinch metoda, je tudi Dupont-Enge-Morain metoda učinkovita za generiranje krivulj s poljubno vključitveno stopnjo k. Za razliko od Cocks-Pinch metode, kjer smo lahko izbrali velikost podgrupe r poljubno, je v Dupont-Enge-Morain metodi število r vrednost polinoma $R(a)$. Ker ima $R(a)$ stopnjo $\varphi(k)$, bodo praštevila r rasla podobno kot $a^{\varphi(k)}$. Lahko pa za število r vzamemo tudi vrednosti praštevilskih faktorjev polinoma $R(a)$ kongruentne 1 $\mod k$. Tudi te vrednosti števila r bodo podobno velike kot vrednosti polinoma $R(a)$, saj bomo izbrali le tiste, ki imajo velikost primerno za uporabo v kriptografiji, če bodo ostali faktorji majhni. Torej imajo možni redi r podgrupe v metodi Dupont-Enge-Morain omejen razpon, kar pa je tudi edina omembe vredna razlika med metodama.

7.6 Redke družine krivulj

Če želimo konstruirati družino krivulj, iščemo polinome $t(x)$, $r(x)$ in $q(x)$, ki zadoščajo definiciji 7.3.5. Povzeto na kratko, polinomi $t(x)$, $r(x)$ in $q(x)$ morajo zadoščati določenim zahtevam glede deljivosti po modulu $r(x)$ in zanje mora imeti enačba kompleksnega množenja za družine $Dy^2 = 4q(x) - t(x)^2$, ki smo jo definirali v (7.3), neskončno celoštevilskih rešitev (x, y). Enačbo lahko napišemo tudi v obliki

$$Dy^2 = 4q(x) - t(x)^2 = 4h(x)r(x) - (t(x) - 2)^2, \tag{7.9}$$

kjer je $h(x)$ kofaktor, ki zadošča enačbi

$$h(x)r(x) = q(x) + 1 - t(x).$$

Če iščemo krivulje, katerih grupa točka bo praštevilske moči, potem postavimo $h(x) = 1$. Miyaji, Nakabayashi in Takano [107] so bili prvi, ki so konstruirali eliptično krivuljo s praštevilskim redom z vnaprej določeno stopnjo vključitve. Njihova konstrukcija je temeljila na dejstvu, da v primeru, ko je desna stran enačbe (7.9) polinom stopnje 2, lahko naredimo substitucijo in enačbo prevedemo v splošno Pellovo enačbo [118]. Take enačbe imajo pogosto neskončno rešitev in v takih primerih lahko dobimo družino krivulj v smislu definicije 7.3.5. Freeman [47] je ta rezultat postavil v bolj splošen kontekst z opazko, da če je $f(x) = 4q(x) - t(x)^2$ desna stran enačbe (7.9) in je polinom $f(x)$ prost kvadratov, potem enačba (7.9) definira gladko afino ravninsko krivuljo rodu $g = \lfloor \frac{\deg(f)-1}{2} \rfloor$. Če je $f(x)$ polinom stopnje 2, potem je $g = 0$ in take krivulje imajo ali nič celih točk (ang. integral point) ali neskončno celih točk. V zadnjem primeru dobimo družino krivulj (t, r, q) v smislu točke 1. definicije 7.3.5. Če pa je $\deg(f) \geq 3$, potem pogoj (e) v točki 1. definicije 7.3.5 nikoli ne more biti izpolnjen [47, trditev 2.10]. V tem primeru ima krivulja definirana z enačbo (7.9) rod $g \geq 1$ in po Siegelovem izreku [137, 37] imajo take krivulje končno mnogo celih točk.

Primer, ko polinom $f(x)$ vsebuje kvadratni faktor, je redek, lahko pa se zgodi [11]. V primeru, ko ima polinom $f(x)$ stopnjo 2 in je prost kvadratov, lahko uporabimo naslednji izrek.

Izrek 7.6.1. *Naj bo $k \in \mathbb{N}$, $t(x) \in \mathbb{Z}[x]$ in $r(x) \in \mathbb{Z}[x]$ nerazcepen faktor ciklotomičnega polinoma $\Phi_k(t(x)-1)$. Potem $\varphi(k) \mid \deg(r)$.*

Dokaz. Naj bo $\deg(t) = d$. Ker je stopnja $\Phi_k(x)$ enaka $\varphi(k)$ iz definicije k-tega ciklotomičnega polinoma A.2.42 sledi $\deg(\Phi_k(t(x)-1)) = d\varphi(k)$. Naj bo ω koren polinoma $r(x)$ in naj bo $\zeta = t(\zeta) - 1$. Potem je $\Phi_k(\zeta) = 0$ in ζ je primitivni k-ti koren enote. Tako imamo naslednje zaporedje obsegov:

$$\mathbb{Q} \subset \mathbb{Q}(\zeta) \subset \mathbb{Q}(\omega).$$

Ker je $[\mathbb{Q}(\omega) : \mathbb{Q}] = \deg(r)$ in $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(k)$, mora $\varphi(k)$ deliti $\deg(r)$. ■

V primeru, ko je $\deg(q) \geq \deg(r)$ in $\varphi(k) \geq 4$, je polinom $4q(x) - t(x)^2$ prost kvadratov in ima stopnjo vsaj 4. Kvadratna desna stran enačbe kompleksnega množenja se lahko izpelje le, če se členi v $4q(x)$ in $t(x)^2$ z visokimi potencami izničijo. Edini tak primer znan do zdaj je za vključitveno stopnjo $k = 10$, za ostale vključitvene stopnje iskanje ustrezne družine $(t(x), r(x), q(x))$ ostaja odprt problem [49].

7.6.1 MNT krivulje

Miyaji, Nakabayashi in Takano [107] so bili prvi, ki so predlagali parjenjem prijazne navadne eliptične krivulje za vključitvene stopnje $k = 3, 4$ in 6. Celotna karakterizacija navadne eliptične krivulje praštevilskega reda s stopnjami vključitve 3,4 ali 6 je podana v naslednjem izreku.

Izrek 7.6.2. *[107]. Naj bo q praštevilo in $E/\mathbb{F}q$ taka navadna eliptična krivulja, da je $r = \#E(\mathbb{F}_q)$ praštevilo večje od 3. Naj bo $t = q + 1 - r$. Potem veljajo naslednje trditve:*

1. *Krivulja E ima vključitveno stopnjo $k = 3$ natanko tedaj, ko obstaja tak $x \in \mathbb{Z}$, da velja $t = -1 \pm 6x$ in $q = 12x^2 - 1$;*
2. *Krivulja E ima vključitveno stopnjo $k = 4$ natanko tedaj, ko obstaja tak $x \in \mathbb{Z}$, da velja $t = -x$ ali $t = x + 1$ in $q = x^2 + x + 1$;*
3. *Krivulja E ima vključitveno stopnjo $k = 6$ natanko tedaj, ko obstaja tak $x \in \mathbb{Z}$, da velja $t = 1 \pm 2x$ in $q = 4x^2 + 1$.*

■

Celotna družina skupaj s polinomom $r(x)$ je v dodatku B.1 v tabeli B.1.1.

Opomba: Karabina in Teske [72, 73] sta dokazala, da v primerih, ko sta r in q obe praštevili večji od 3, obstaja eliptična krivulja $E/\mathbb{F}_q$ z vključitveno stopnjo 6, diskriminanto D in $\#E(\mathbb{F}_q) = r$ natanko tedaj, ko obstaja eliptična krivulja $E'/\mathbb{F}_r$ z vključitveno stopnjo 4, diskriminanto D in $\#E'(\mathbb{F}_r) = q$.

V vseh treh primerih izreka 7.6.2 enačba kompleksnega množenja $Dy^2 = 4q(x) - t(x)^2$ definira krivuljo roda nič, kjer je desna stran enačbe kvadratna v x. V vseh primerih lahko z linearno spremembo spremenljivk enačbo prevedemo v splošno Pellovo enačbo oblike

$$X^2 - SDY^2 = M. \tag{7.10}$$

V posebnem velja:

1. Za $k = 3$ z uvedbo nove spremenljivke $X = 6x \pm 3$ enačbo $Dy^2 = 4q(x) - t(x)^2$ prevedemo v enačbo $X^2 - 3Dy^2 = 24$;

2. Za $k = 4$ z uvedbo nove spremenljivke $X = 3x \pm 2$, če je $t = -x$ in $X = 3x + 1$ če je $t = x + 1$, enačbo $Dy^2 = 4q(x) - t(x)^2$ prevedemo v $X^2 - 3Dy^2 = -8$;

3. Za $k = 6$ z uvedbo nove spremenljivke $X = 6x \pm 1$ enačbo $Dy^2 = 4q(x) - t(x)^2$ prevedemo v $X^2 - 3Dy^2 = -8$.

Predznaki $\pm$ se ujemajo s predznaki v izreku 7.6.2. Reševanje Pellove enačbe je opisano v [118, 92].

MNT strategija za generiranje navadnih eliptičnih krivulj praštevilskega reda z vključitveno stopnjo $k = 3, 4$ ali 6 je naslednja:

1. Ponavljajoče izbirajmo majhno diskriminanto D in izračunajmo rešitve pripadajoče Pellove enačbe, dokler pripadajoči vrednosti $q = q(x)$ in $r = q(x) + 1 - t(x)$ nista praštevili zaželene dolžine (v bitih);

2. Ko dobimo vrednosti v koraku 1., obstaja eliptična krivulja nad obsegom $\mathbb{F}_q$ z r točkami in vključitveno stopnjo 3, 4, ali 6, ki se lahko konstruira z metodo kompleksnega množenja.

Iskanje MNT krivulj lahko še pospešimo, če uporabimo dejstvo, da je pri $k = 3$ potreben pogoj $D \equiv 19 \pmod{24}$ in da je pri $k = 4, 6$ potreben pogoj $D \not\equiv 5 \pmod{10}$ [107]. Poleg tega mora biti v vseh treh primerih vrednost M v enačbi (7.10) kvadratni ostanek po modulu $3D$.

Glavna slabost MNT krivulj je v tem, da lahko zaporedne rešitve (X_j, Y_j) splošne Pellove enačbe rastejo eksponentno in tako dobimo le nekaj ustreznih x-vrednosti in s tem redko družino glede na definicijo 7.3.5. Obstajajo hevristični argumenti [95], da za vsako zgornjo mejo $\overline{D}$ obstaja končno mnogo krivulj MNT z diskriminanto $D \leq \overline{D}$ brez omejitev glede na velikost obsega. Po drugi strani, pa so bile konstruirane specifične MNT krivulje, ki so zanimive za kriptografijo [116, 135].

7.6.2 GMT krivulje

MNT strategijo opisano v prejšnjem razdelku so razširili Scott in Baretto [136] ter Galbraith, McKee in Valença [55] (GMT krivulje) z uporabo majhnega konstantnega kofaktorja h.

Scott in Baretto [136] sta fiksirala majhni celi števili h in d, zamenjala $r = \Phi_k(t-1)/d$ in $t = x + 1$ v enačbi (7.9) ter tako dobila enačbo kompleksnega množenja oblike

$$Dy^2 = 4h\frac{\Phi_k(x)}{d} - (x-1)^2. \tag{7.11}$$

Pri tem sta uporabila dejstvo, da je $\Phi_k(t-1) \equiv 0 \pmod{r}$. Ker je podobno kot pri MNT krivuljah tudi tu desna stran enačbe kvadratna v x pri $k = 3, 4$ ali 6, lahko enačbo (7.11) prevedemo v splošno Pellovo enačbo s primerno linearno substitucijo za x. Scott in Baretto sta našla rešitve za tako prevedene Pellove enačbe za majhen D in poljuben y z omejitvijo $4h \geq d$.

Galbraith, McKee in Valença [55] so podali kompletno karakterizacijo krivulj z vključitveno stopnjo $k = 3, 4$ in 6 in kofaktorjem $2 \leq h \leq 5$. To so dosegli tako, da so pri MNT dokazu izreka 7.6.2 za moč $\#E(\mathbb{F}_q)$ namesto r vzeli produkt hr in nato eksplicitno analizirali primere, ko je $h = 2, 3, 4, 5$. Kot v primeru $\#E(\mathbb{F}_q) = r$, so vse parametrizacije za število t linearni polinomi v x in vse parametrizacije za število q kvadratni polinomi v x. Pripadajoče enačbe kompleksnega množenja $Dy^2 = 4q(x) - t(x)^2$ so kvadratni polinomi spremenljivke x in se lahko prevedejo na splošne Pellove enačbe. Njihovi rezultati za polinome $q(x)$ in $t(x)$ so v tabeli B.2.1.

7.6.3 LMT krivulje

Le, Mrabet in Tan [88] so dodatno izboljšali rezultate Galbraith, McKee in Valença tako, da so razvili enostaven in ekspliciten algoritem 7.6.1 za iskanje družin krivulj. Rezultati za polinome $q(x)$, $r(x)$ in $t(x)$ izračunane s tem algoritmom so v tabeli B.3.1. Njihove konstrukcije v originalni taksonomiji [49] ni bilo, dodali smo jo kot poseben primer redkih družin.

Algoritem 7.6.1 Algoritem za konstrukcijo LMT družin krivulj

Vhodni podatki: vključitvena stopnja k in kofaktor $h_{\max}$;
Rezultat: seznam polinomov $\{t(x), r(x), q(x)\}$;
$L \leftarrow \{\}$, $T \leftarrow \{\}$;
for $a = -4h_{\max}$, $a \leq 4h_{\max}$ **do**
  for $b = -4h_{\max} + 1$, $b \leq 4h_{\max} - 1$ **do**
    $t(x) \leftarrow ax + b$;
    $f(x) \leftarrow \Phi_k((t(x) - 1)$;
    $f(x) = d \cdot r(x)$, kjer je $d \in \mathbb{Z}$ in $r(x)$ nerazcepen kvadraten polinom;
    if par $((t(x), r(x))$ ne moremo transformirati v noben par $(t'(x), r'(x))$ v T s spremembo $x \mapsto cx + d$, $c, d \in \mathbb{Z}$ **then**
      $T \leftarrow T + \{(d, t(x), r(x))\}$;
      for $h = \lceil d/4 \rceil$, $h \leq h_{\max}$ **do**
        $q(x) \leftarrow h \cdot r(x) + t(x) - 1$;
        if $q(x)$ nerazcepen in $\gcd(q(x), r(x) : x \in \mathbb{Z}) = 1$ **then**
          $L \leftarrow L + \{(t(x), r(x), q(x), h\}$;
        end if
      end for
    end if
  end for
end for
return L.

S pomočjo zgornjega algoritma ne konstruiramo krivulj z manjšo vrednostjo ρ, kot v primeru MNT ali GMT krivulj. Vendar pa je algoritem zaradi eksplicitnosti zanimiv za implementacijo in zaradi tega obstaja tudi prosto dosegljiva implementacija tega algoritma za programski paket Magma [88].

7.6.4 Freeman-ova družina za $k = 10$

Kot smo omenili že na strani 112, je v primeru, ko je $\varphi(k) > 2$, verjetnost, da je desna stran enačbe (7.9) kvadratna zelo majhna. Freeman [47] je odkril primer, ko se to zgodi za vključitveno stopnjo $k = 10$. Njegova konstrukcija krivulje uporabi naslednjo faktorizacijo ciklotomičnega polinoma $\Phi_{10}(u(x))$, kjer je $u(x) = 10x^2 + 5x + 2$ [55]:

$$\Phi_{10}(u(x)) = (25x^4 + 25x^3 + 15x^2 + 5x + 1) \cdot (400x^4 + 400x^3 + 240x2 + 60x + 11).$$

Z uporabo te faktorizacije in z uporabo naslednjih polinomov za $t(x), r(x), q(x)$:

$$\begin{array}{lcll} r(x) & & = & 25x^4 + 25x^3 + 15x^2 + 5x + 1, \\ t(x) & = & u(x) + 1 & = 10x^2 + 5x + 3, \\ q(x) & = & r(x) + t(x) - 1 & = 25x^4 + 25x^3 + 25x^2 + 5x + 1, \end{array}$$

se člena polinoma $f(x) = 4q(x) - t(x)^2$ z najvišjimi potencami krajšata in rezultat je kvadratna enačba kompleksnega množenja $Dy^2 = 15x^2 + 10x + 3$. S substitucijo $X = 15x + 5$ je ta enačba kompleksnega množenja ekvivalentna splošni Pellovi enačbi $X^2 - 15Dy^2 = -20$. Za vsako vrednost $D \in \mathbb{N}$, za katere ima ta enačba celoštevilske rešitve, taka izbira generira redko družino krivulj (t, r, q) z vključitveno stopnjo $k = 10$. Krivulje lahko izračunamo s posnemanjem MNT strategije in upoštevanjem dejstva, da mora vsako število D, ki pripelje do rešitve, ustrezati pogojema $D \equiv 43 \pmod{120}$ ali $D \equiv 67 \pmod{120}$.

7.7 Polne družine krivulj

Naj bo

$$Dy^2 = 4q(x) - t(x)^2 = 4h(x)r(x) - (t(x) - 2)^2 \tag{7.12}$$

enačba kompleksnega množenja. Poiskati moramo polinome $t(x)$, $r(x)$ in $q(x)$, ki zadoščajo določenim kriterijem deljivosti in za katere ima enačba kompleksnega množenja (7.12) neskončno mnogo rešitev (x, y). V tem razdelku bomo konstruirali krivulje z ustrezno izbiro parametrov D, $t(x)$, $r(x)$ in $q(x)$, tako da bo desna stran enačbe (7.12) vedno enaka produktu števila D in kvadrata polinoma $y(x)$. Take konstrukcije nam bodo dale polno družino krivulj po točki 4. definicije 7.3.5.

Obstajata dve glavni strategiji za generiranje polnih družin krivulj. Avtorja prve sta Scott in Baretto [136], avtorji druge pa originalno Barreto, Lynn in Scott [9] ter posplošitve Brezing in Weng [25]. Obe strategiji začneta podobno:

1. Fiksirajmo vključitveno stopnjo k;

2. Izberimo tak nerazcepen polinom $r(x) \in \mathbb{Z}[x]$, da je obseg $K \cong \mathbb{Q}[x]/(r(x))$ številski obseg, ki vsebuje k-te korene enote;

3. Izberimo polinom $t(x) \in \mathbb{Q}[x]/(r(x))$ kot polinom, ki ga izomorfizem obsegov $\mathbb{Q}[x]/(r(x)) \to K$ preslika v element $1 + \zeta_k \in K$, kjer je ζ_k primitivni k-ti koren enote v K.

Izomorfizem v točki 3. zgoraj obstaja, saj sta si obsega K in $\mathbb{Q}[x]/(r(x))$ izomorfna. V nadaljevanju bomo tako izbranemu polinomu rekli, da **ustreza elementu obsega**. Seveda velja tudi obratno, lahko izberemo element $a \in K$, ki ga obrat izomorfizma v točki 2. preslika v nek vnaprej izbrani polinom $f(x) \in \mathbb{Q}[x]/(r(x))$. V tem primeru bomo tako izbranemu elementu obsega K rekli, da **ustreza polinomu**.

Po teh korakih, pa se strategiji razlikujeta. Brezing in Weng uporabita naslednje dejstvo: če obseg K vsebuje $\sqrt{-D}$, lahko enačbo kompleksnega množenja (7.12) zaradi $r(x) = 0$ v $K = \mathbb{Q}[x]/(r(x))$ faktoriziramo v K in dobimo

$$(t(x) - 2 + y\sqrt{-D})(t(x) - 2 - y\sqrt{-D}) \equiv 0 \pmod{r(x)}.$$

Ker izbrani polinom $t(x)$ ustreza elementu $\zeta_k + 1$, za $y(x)$ izberemo polinom, ki ustreza elementu $(\zeta_k - q)/\sqrt{-D} \in K$. Pri tako izbranem polinomu $y(x)$ je enačbi (7.12) zadoščeno za vsak $x \in \mathbb{Z}$ [25]. V primeru, ko ne vemo, ali K vsebuje element oblike $\sqrt{-D}$ za nek majhen $D \in \mathbb{N}$, uporabimo Scott-Barreto strategijo. Pri tej izberemo polinoma $t(x)$ in $r(x)$ kot je opisano v točkah 2. in 3. zgoraj (skupni koraki), nato poiščemo kofaktorje $h(x)$, ki zagotovijo, da je desna stran enačbe kompleksnega množenja (7.12) ali popoln kvadrat ali produkt popolnega kvadrata in linearnega faktorja. Take kofaktorje najdemo z računalnikom [49]. Enačba kompleksnega množenja (7.12) se tako prevede v naslednjo enačbo

$$Dy^2 = (ax + b)g(x)^2.$$

Če je $a = 0$ vzamemo $D = b$ in $y = g(x)$. Če pa je $a > 0$ pa lahko za D vzamemo poljubno naravno število in s spremembo spremenljivk $x \mapsto (Dz^2 - b)/a$ in $y \mapsto zg(x)$ enačba kompleksnega množenja zadošča za vsak $z \in \mathbb{Z}$.

V obeh primerih konstruiramo polinom $q(x)$ kot

$$q(x) = \frac{1}{4}(t(x)^2 + Dy(x)^2).$$

Če $q(x)$ predstavlja praštevilo in ima $r(x)$ pozitivni vodilni koeficient, potem trojica (t, r, q) parametrizira polno družino parjenjem prijaznih krivulj.

Uspeh zgoraj opisanih strategij je odvisen od izbire številskega obsega K. Najbolj očitna izbira za K je ciklotomični obseg $\mathbb{Q}(\zeta_\ell)$ za nek ℓ, ki je večkratnik vključitvene stopnje k. V tem primeru je polinom $r(x)$ kar ℓ-ti ciklotomični polinom $\Phi_\ell(x)$. Tako izbran obseg K vsebuje k-te korene enot. V posebnem, če $4 \mid \ell$ obseg K vsebuje $\sqrt{-1}$, če $8 \mid \ell$ obseg K vsebuje $\sqrt{-2}$ in za vsako liho praštevilo p, ki deli ℓ, obseg K vsebuje $\sqrt{\left(\frac{-1}{p}\right) p}$. V Brezing-Weng konstrukciji lahko za poljubno vključitveno stopnjo $k \in \mathbb{N}$ in diskriminanto $D \in \mathbb{N}$ uporabimo ciklotomičen obseg in zaradi tega takim družinam pravimo tudi **ciklotomične družine**. Podrobneje si jih bomo ogledali v razdelku 7.7.1.

Še boljše rezultate dobimo, če za obseg K izberemo razširitev ciklotomičnega obsega, za $r(x) \in \mathbb{Z}[x]$ pa izberemo nerazcepni polinom, ki ni ciklotomičen. Tako razširitev lahko konstruiramo na naslednja načina:

1. Izračunamo ciklotomični polinom Φ_ℓ za nek polinom $u(x)$. Če je $\Phi_\ell(u(x))$ nerazcepen, nismo dosegli ničesar. V primeru, ko je $\Phi_\ell(u(x)) = r_1(x)r_2(x)$, kjer je $r_1(x)$ nerazcepen, pa vzamemo za obseg $K = \mathbb{Q}[x]/(r_1(x))$. V tem primeru je K obseg,

ki vsebuje ℓ-te korene enote in polinom $u(x)$ ustreza ℓ-tem korenu enote v obsegu K. Če vemo, da je $\sqrt{-D} \in \mathbb{Q}(\zeta_\ell)$, potem je tudi $\sqrt{-D} \in K$ in lahko uporabimo Brezing-Weng konstrukcijo, drugače uporabimo Scott-Barreto konstrukcijo.

2. Avtorji druge konstrukcije so Kachisa, Schaefer in Scott [71]. Poiščemo tak neciklotomični nerazcepen polinom $r(x)$, da je $K = \mathbb{Q}[x]/(r(x))$ izomorfen ciklotomičnem obsegu $\mathbb{Q}(\zeta_\ell)$ za nek $\ell \in \mathbb{N}$. Polinom $r(x)$ lahko izračunamo kot minimalen polinom naključnega elementa iz obsega $\mathbb{Q}(\zeta_\ell)$. Tak $r(x)$ uporabimo za izračun polinoma $z(x) \in \mathbb{Q}[x]/(r(x))$, ki ustreza elementu $\zeta_\ell \in K$, in nato uporabimo Brezing-Weng konstrukcijo.

Ker je netrivialen razcep polinoma $\Phi_\ell(u(x))$ za naključen $u(x)$ redek, poleg tega pa polinom $q(x)$ generiran po Kachisa-Schaefer-Scott metodi ponavadi ne predstavlja praštevil, družinam krivulj dobljenih s postopkom v točki 2. zgoraj, pravimo **sporadične družine** [49] in si jih bomo ogledali v razdelku 7.7.2.

7.7.1 Ciklotomične družine krivulj

Barreto, Lynn in Scott [9] ter neodvisno Brezing in Weng [25] so opazili, da lahko z uporabo polinomov kot parametrov t, r, q izboljšamo vrednost ρ krivulje definirane v (7.7), ki je za krivulje generirane s Cocks-Pinch metodo blizu 2. Brezing in Weng sta konstrukcijo najbolj posplošila in njuni rezultati so strnjeni v naslednjem izreku.

Izrek 7.7.1. *[25]. Fiksirajmo naravno število k in naravno število prosto kvadratov D.*

1. *Naj bo $r(x) \in \mathbb{Z}[x])$ tak nerazcepen polinom s pozitivnim vodilnim koeficientom, da je $K = \mathbb{Q}[x]/(r(x))$ številski obseg, ki vsebuje $\sqrt{D}$ in ciklotomičen obseg $\mathbb{Q}(\zeta_k) \subseteq K$.*
2. *Naj bo $\zeta_k \in K$ primitivni k-ti koren enote.*
3. *Naj bo $t(x) \in \mathbb{Q}[x]$ polinom, ki ustreza elementu $\zeta_k + 1$ v obsegu K.*
4. *Naj bo $y(x) \in \mathbb{Q}[x]$ polinom, ki ustreza elementu $(\zeta_k - 1)/\sqrt{D}$ v obsegu K (če $\sqrt{D}$ ustreza polinomu $s(x)$, potem je $y(x) \equiv (2 - t(x))s(x)/D \mod r(x)$).*
5. *Naj bo $q(x) \in \mathbb{Q}[x]$ podan z $(t(x)^2 + Dy(x)^2)/4$.*

Če $q(x)$ predstavlja praštevila, potem trojka $(t(x), r(x), q(x))$ parametrizira polno družino eliptičnih krivulj z vključitveno stopnjo k in diskriminanto D. Vrednost ρ te družine je enaka

$$\rho(t, r, q) = \frac{2 \max\{\deg t(x), \deg y(x)\}}{\deg r(x)}. \tag{7.13}$$

■

Ker polinoma $t(x)$ in $y(x)$ lahko vedno izberemo tako, da imata stopnjo strogo manjšo od stopnje polinoma $r(x)$, metoda po zgornjem izreku generira družino krivulj z vrednostjo ρ strogo manjšo od 2. V večini primerov je vrednost ρ malo manjša od 2, s primerno izbiro obsega K pa jo lahko še zmanjšamo [49]. V nadaljevanju si bomo ogledali nekaj primerov konstrukcij, ki temeljijo na izreku 7.7.1.

Prva konstrukcija je Brezing-Weng konstrukcija [25]. Za obseg K si bomo izbrali ciklotomični obseg, ki vsebuje četrti koren enote $\sqrt{-1}$, tako da za D lahko izberemo $D = 1$.

Konstrukcija 7.7.2. *Naj bo k liho naravno število, $k < 1000$. Definirajmo:*

$$\begin{aligned} r(x) &= \Phi_{4k}(x), \\ t(x) &= -x^2 + 1, \\ q(x) &= (x^{2k+4} + 2x^{2k+2} + x^{2k} + x^4 - 2x^2 + 1)/4. \end{aligned} \tag{7.14}$$

Trojka (t, r, q) parametrizira polno družino eliptičnih krivulj z vključitveno stopnjo k in diskriminanto $D = 1$ glede na definicijo 7.3.5. Vrednost ρ te družine je $(k + 2)/\varphi(k)$.

Dokaz. Uporabimo izrek 7.7.1 za izbrani obseg $K = \mathbb{Q}[x]/(r(x)) \cong \mathbb{Q}(\zeta_{4k})$. Po lemi A.2.38 je $\mathbb{Q}(\zeta_k) \subseteq K$ in $\mathbb{Q}(\zeta_4) \subseteq K$, posledično K vsebuje tudi $\sqrt{-1}$. Naj element ζ_k ustreza polinomu $-x^2$ in naj element $\sqrt{-1}$ ustreza polinomu x^k. Ker obseg K vsebuje $\sqrt{-D} = \sqrt{-1}$, po izreku 7.7.1 za $y(x)$ izberemo polinom, ki ustreza elementu $(\zeta_k - 1)/\sqrt{-1} \in K$. Tako je $y(x) = (x^2 + 1)x^k$ in $q(x) = ((-x^2 + 1)^2 + (x^2 + 1)^2x^{2k})/4$, ki se poenostavi v polinom $q(x)$ iz (7.14). Vrednosti $q(x)$ so za lihe x cela števila in $q(1) = 1$. Če je polinom q nerazcepen, potem predstavlja praštevila (glej opombo na strani 104). Z računalnikom se da pokazati, da je za lihe $k < 1000$ polinom $q(x)$ nerazcepen [24, 49]. Poleg tega velja še $y(x) \in \mathbb{Z}$ za $x \in \mathbb{Z}$ in če uporabimo (7.13) v izreku 7.7.1 ter dejstvo, da je $\deg(r) = 2\varphi(k)$ in $\deg(t) < \deg(y) = k + 2$, dobimo vrednost $\rho = (k + 2)/\varphi(k)$. ■

Če je k liho število, potem velja $\zeta_{2k} = -\zeta_k$ [93]. Če spremenimo predznake v polinomskih predstavitvah ζ_k v konstrukciji 7.7.2, lahko uporabimo enako konstrukcijo za generiranje družine krivulj z vključitveno stopnjo $2k$ in z enako vrednostjo ρ.

Konstrukcija 7.7.3. *Naj bo k liho naravno število, $k < 1000$. Definirajmo:*

$$\begin{aligned} r(x) &= \Phi_{4k}(x), \\ t(x) &= x^2 + 1, \\ q(x) &= (x^{2k+4} - 2x^{2k+2} + x^{2k} + x^4 + 2x^2 + 1)/4. \end{aligned}$$

Trojka (t, r, q) parametrizira polno družino eliptičnih krivulj z vključitveno stopnjo $k' = 2k$ in diskriminanto $D = 1$ glede na definicijo 7.3.5. Vrednost ρ te družine je $(k'/2+2)/\varphi(k')$.

Dokaz. Podobno kot v dokazu konstrukcije 7.7.2 naj elementa $\sqrt{-1}$ in ζ_{2k} obsega $K = \mathbb{Q}[x]/(r(x))$ ustrezata polinomoma x^k in x^2 zaporedoma. Z izbiro $y(x) = (-x^2 + 1)x^k$ dobimo polinom $q(x)$ iz konstrukcije 7.7.3. Podobno kot v dokazu konstrukcije 7.7.2, tudi tu velja $q(1) = 1$ in $q(x) \in \mathbb{Z}$ za $x \in \mathbb{Z}$ in x liho število. Polinom $q(x)$ v 7.7.3 je nerazcepen natanko tedaj, ko je nerazcepen polinom $q(x)$ iz konstrukcije 7.7.2 in podobno kot v konstrukciji 7.7.2 je vrednost ρ te družine po (7.13) enaka $(k + 2)/\varphi(k)$. ■

Če uporabimo lastnost primitivnih korenov enote $\zeta_{4k} = \sqrt{\zeta_{2k}}$, dobimo naslednjo konstrukcijo.

Konstrukcija 7.7.4. *Naj bo k liho število, $k < 1000$. Definirajmo:*

$$\begin{aligned} r(x) &= \Phi_{4k}(x), \\ t(x) &= x + 1, \\ q(x) &= (x^{2k+2} - 2x^{2k+1} + x^{2k} + x^2 + 2x + 1)/4. \end{aligned}$$

Trojka (t, r, q) parametrizira polno družino eliptičnih krivulj z vključitveno stopnjo $k' = 4k$ in diskriminanto $D = 1$ glede na definicijo 7.3.5. Vrednost ρ te družine je enaka $(k'/2 + 2)/\varphi(k')$.

Dokaz. Zopet uporabimo izrek 7.7.1. Naj elementa $\sqrt{-1}$ in ζ_{4k} obsega $K = \mathbb{Q}[x]/(r(x))$ ustrezata polinomoma x^k in x zaporedoma. Z izbiro $y(x) = (-x + 1)x^k$ dobimo polinom $q(x)$ iz konstrukcije 7.7.4. Podobno kot v dokazu konstrukcije 7.7.2, tudi tu velja $q(1) = 1$. Ker je $q(x)$ nerazcepen za liha cela števila $k < 1000$ (to dokažemo z računalnikom [24, 49]), polinom $q(x)$ iz konstrukcije 7.7.4 predstavlja praštevila. Vrednost ρ te družine je po (7.13) enaka $(k + 1)/\varphi(k)$. ■

Za vključitveno stopnjo $k = 10$ uporabimo posebno Brezing-Weng konstrukcijo [25], da dobimo boljšo vrednost ρ.

Konstrukcija 7.7.5. *Naj bo $k = 10$. Definirajmo:*

$$\begin{aligned} r(x) &= \Phi_{20}(x) = x^8 - x^6 + x^4 - x^2 + 1, \\ t(x) &= -x^6 + x^4 - x^2 + 2, \\ q(x) &= (x^{12} - x^{10} + x^8 - 5x^6 + 5x^4 - 4x^2 + 4)/4. \end{aligned}$$

Trojka (t, r, q) parametrizira polno družino eliptičnih krivulj z vključitveno stopnjo 10 in diskriminanto $D = 1$ glede na definicijo 7.3.5. Vrednost ρ te družine je enaka $3/2$.

Dokaz. Obseg $K = \mathbb{Q}[x]/(r(x)) \cong \mathbb{Q}(\zeta_{20})$ po lemi A.2.38 vsebuje elementa ζ_{10} in $\sqrt{-1}$. Če elementa $\sqrt{-1}$ in ζ_{10} obsega K ustrezata polinomoma x^5 in $-x^6+x^4-x^2+1$ zaporedoma, potem po izreku 7.7.1 element $\zeta_{10} + 1$ ustreza polinomu $t(x)$ in z izbiro $y(x) = x^5 - x^3$ dobimo $q(x)$ iz konstrukcije 7.7.5. Ker je $q(0) = 1$ in $q(x)$ nerazcepen nad $\mathbb{Z}$ (preverimo z računalnikom), $q(x)$ predstavlja praštevilo. Vrednost ρ te družine je po (7.13) enaka $3/2$. ■

Zdaj si bomo za K izbrali ciklotomični obseg, ki vsebuje kubični koren enote. Taki obsegi po lemi A.2.41 vsebujejo tudi $\sqrt{-3}$, tako da za diskriminanto lahko izberemo $D = 3$. V nadaljevanju si bomo ogledali družine (oziroma potencialne družine) eliptičnih krivulj glede na definicijo 7.3.5 za vse vrednosti vključitvene stopnje k, ki niso deljive z 18.

Konstrukcija 7.7.6. *Naj bo $k \in \mathbb{N}$, $k \leq 1000$ in $18 \nmid k$.*

1. *Če je $k \equiv 1 \pmod 6$, definirajmo:*

$$\begin{aligned} r(x) &= \Phi_{6k}(x), \\ t(x) &= -x^{k+1} + x + 1, \\ q(x) &= \tfrac{1}{3}(x + 1)^2(x^{2k} - x^k + 1) - x^{2k+1}. \end{aligned}$$

2. *Če je $k \equiv 2 \pmod 6$, definirajmo:*

$$\begin{aligned} r(x) &= \Phi_{3k}(x), \\ t(x) &= x^{k/2+1} - x + 1, \\ q(x) &= \tfrac{1}{3}(x - 1)^2(x^k - x^{k/2} + 1) + x^{k+1}. \end{aligned}$$

3. *Če je* $k \equiv 3 \pmod 6$, *definirajmo:*

$$\begin{aligned} r(x) &= \Phi_{2k}(x), \\ t(x) &= -x^{k/3+1} + x + 1, \\ q(x) &= \tfrac{1}{3}(x+1)^2(x^{2k/3} - x^{k/3} + 1) - x^{2k/3+1}. \end{aligned}$$

4. *Če je* $k \equiv 4 \pmod 6$, *definirajmo:*

$$\begin{aligned} r(x) &= \Phi_{3k}(x), \\ t(x) &= x^3 + 1, \\ q(x) &= \tfrac{1}{3}(x^3-1)^2(x^k - x^{k/2} + 1) + x^3. \end{aligned}$$

5. *Če je* $k \equiv 5 \pmod 6$, *definirajmo:*

$$\begin{aligned} r(x) &= \Phi_{6k}(x), \\ t(x) &= x^{k+1} + 1, \\ q(x) &= \tfrac{1}{3}(x^2 - x + 1)(x^{2k} - x^k + 1) + x^{k+1}. \end{aligned}$$

6. *Če je* $k \equiv 0 \pmod 6$, *definirajmo:*

$$\begin{aligned} r(x) &= \Phi_k(x), \\ t(x) &= x + 1, \\ q(x) &= \tfrac{1}{3}(x-1)^2(x^{k/3} - x^{k/6} + 1) + x. \end{aligned}$$

Trojka (t, r, q) *parametrizira polno družino eliptičnih krivulj z vključitveno stopnjo* k *in diskriminanto* $D = 3$ *glede na definicijo 7.3.5. Naj bo* ℓ *najmanjši skupni večkratnik števil* 6 *in* k. *Če je* $k \equiv 4 \pmod 6$ *je vrednost* ρ *vsake take družine* $\rho = (\ell/3 + 6)/\varphi(\ell)$, *sicer pa* $\rho = (\ell/3 + 2)/\varphi(\ell)$. *Za vse* $k \leq 1000$, *razen za* $k = 4$, *je vrednost* $\rho \leq 2$ *in za vse* $5 \leq k \leq 1000$, *razen za* $k = 6$ *in* $k = 10$, *je vrednost* $\rho < 2$.

Dokaz. Podobno kot v prejšnjih konstrukcijah, bomo tudi tu uporabili izrek 7.7.1 in za polinom $r(x)$ izbrali ciklotomični polinom $\Phi_\ell(x)$, kjer je $\ell = \operatorname{lcm}(k, 6)$. Delamo v obsegu $\mathbb{Q}(\zeta_k, \zeta_6) = \mathbb{Q}(\zeta_{\operatorname{lcm}(k,6)})$, ki je izomorfen obsegu $K = \mathbb{Q}[x]/(\Phi_\ell(x))$. Naj element $\sqrt{-3}$ ustreza polinomu $2x^{\ell/6} - 1$. Naš cilj je najti polinom $y(x)$ majhne stopnje, tako da bo element $(\zeta_k - 1)/\sqrt{-3}$ ustrezal polinomu $y(x)$. Stopnja polinoma $y(x)$ bo odvisna od izbire polinoma $z(x)$, ki ustreza elementu ζ_k. Najbolj očitna izbira je $z(x) = x^{\ell/k}$, vendar je v mnogih primerih boljša izbira $z(x) = x^a \pmod{\Phi_\ell(x)}$, kjer je a malo večji od $\ell/6$. Če polinom x ustreza primitivnemu ℓ-temu korenu enote, mora za a veljati, da je večkratnik ℓ/k in $\gcd(a, k) = 1$. V tem primeru bo polinom x^a ustrezal primitivnemu k-temu korenu enote. Točne izbire za polinom $z(x)$ so podane spodaj. Za tako izbrani polinom $z(x)$ definiramo $t(x) = z(x) + 1$ in polinom $y(x)$ izračunamo kot $\frac{1}{3}(z(x) - 1)(1 - 2x^{\ell/6})$, ki mu dodamo še člen $\pm\frac{2}{3}x\Phi_6(x^{\ell/k})$ (polinom deljiv z $r(x)$) z namenom, da izničimo vodilni člen v primerih, ko je $k \mod 6 \in \{1, 2, 3, 5\}$. Natančneje:

1. Če je $k \equiv 1 \pmod 6$, potem je $\ell = 6k$ in ker $2k + 1 \equiv 3 \pmod 6$, polinom x^{2k+1} ustreza primitivnemu $2k$-temu korenu enote. Ker je k liho število, polinom $-x^{2k+1}$ ustreza primitivnemu k-temu korenu enote. V tem primeru izberemo $z(x) = -x^{2k+1} \equiv -x^{k+1} + x \mod r(x)$. Taka izbira nam da polinom $t(x)$ kot je v točki 1. konstrukcije 7.7.6 in $y(x) = (-x^{k+1} + 2x^k - x - 1)/3$.

2. Če je $k \equiv 2 \pmod 6$, potem je $\ell = 3k$. Ker je $k+1 \equiv 3 \pmod 6$ izberemo $z(x) = x^{k+1} \equiv x^{k/2+1} - x \mod r(x)$. Taka izbira nam da polinom $t(x)$ kot je v točki 2. konstrukcije 7.7.6 in $y(x) = (x^{k/2+1} + 2x^{k/2} + x - 1)/3$.

3. Če je $k \equiv 3 \pmod 6$, potem je $\ell = 2k$. Ker polinom $x^{2k/3}$ ustreza kubičnemu korenu enote in $3 \mid k$, moramo polinom $x^{2k/3}$ pomnožiti s polinomom, ki ustreza primitivnemu k-temu korenu enote. Ker je k liho število in polinom x ustreza $2k$-temu korenu enote, polinom $-x$ ustreza k-temu korenu enote. Izberemo $z(x) = -x^{2k/3+1} \equiv -x^{k/3+1} + x \pmod{r(x)}$. Taka izbira nam da polinom $t(x)$ kot je v točki 3. v konstrukciji 7.7.6 in $y(x) = (-x^{k/3+1} + 2x^{k/3} - x - 1)/3$.

4. Če je $k \equiv 4 \pmod 6$, potem je $\ell = 3k$. Izberemo $z(x) = x^3$ in izračunamo $y(x) = (-2x^{k/2+3} + 2x^{k/2} + x^3 - 1)/3$.

5. Če je $k \equiv 5 \pmod 6$, potem je $\ell = 6k$. Ker je $k+1 \equiv 0 \pmod 6$, izberemo $z(x) = x^{k+1}$ in izračunamo $y(x) = (-x^{k+1} + 2x^k + 2x - 1)/3$.

6. Če je $k \equiv 0 \pmod 6$, potem je $\ell = k$. Izberemo $z(x) = x$ in izračunamo $y(x) = (-2x^{k/6+1} + 2x^{k/6} + x - 1)/3$.

Z izračunom $q(x) = (t(x)^2 + 3y(x)^2)/4$ lahko hitro preverimo, da z zgoraj izbranimi polinomi $t(x)$ in $y(x)$ dobimo polinome $q(x)$ v konstrukciji 7.7.6. Za majhne vrednosti števila k nekateri od tako izračunanih $t(x)$ in $y(x)$ niso popolnoma reducirani po modulu $r(x)$. V takih primerih nadaljnja redukcija pripelje do polinoma $q(x)$, ki ne predstavlja praštevil.

Ostane nam preveriti samo še, ali polinom $q(x)$ predstavljaj praštevila. Pogoja 4. in 5. definicije 7.3.3 lahko preverimo hkrati. Če je k sodo število, potem je $q(1) = 1$, če je $k \equiv 1 \pmod 6$ ali $k \equiv 3 \pmod 6$, potem je $q(-1) = 1$. Če je $k \equiv 5 \pmod 6$, potem je $q(-1) = 4$ in je $q(2)$ liho število. Z računalnikom [24, 49] lahko dokažemo, da je primeren polinom $q(x)$ nerazcepen za vsak $k \leq 1000$, razen za tiste k, ki so deljivi z 18. Zato v izreku tudi zahtevamo $k \nmid 18$.

Za izračun vrednosti ρ uporabimo (7.13) in dejstvo, da je $\deg(q) = \ell/3 + 2$ v vseh primerih, razen $k \equiv 4 \pmod 6$, kjer je $\deg(q) = \ell/3 + 6$.

■

Naslednja izbira za obseg K bo ciklotomični obseg, ki vsebuje osmi koren enote. Taki obsegi vsebujejo $\sqrt{-2}$, zato lahko izberemo za diskriminanto $D = 2$. Prvo konstrukcijo v takem obsegu za vključitveno stopnjo $k = 24$ sta podala Murphy in Fitzpatrick [110]. Mi si bomo ogledali podobno konstrukcijo za vsak k, ki je deljiv s 3.

Konstrukcija 7.7.7. *Naj bo $k \in \mathbb{N}$, $k < 1000$ in $3 \mid k$. Naj bo $\ell = \operatorname{lcm}(8, k)$. Definirajmo:*

$$\begin{aligned} r(x) &= \Phi_l(x), \\ t(x) &= x^{l/k} + 1, \\ q(x) &= \left(2(x^{l/k}+1)^2 + (1 - x^{l/k})^2(x^{5l/24} + x^{l/8} - x^{l/24})^2\right)/8. \end{aligned}$$

Trojka (t, r, q) parametrizira polno družino krivulj z vključitveno stopnjo k in diskriminanto $D = 2$ glede na definicijo 7.3.5. Če je k liho število, je vrednost $\rho = (4 + 5k/6)/\varphi(k)$, če je k sodo število je vrednost $\rho = (2 + 5k/12)/\varphi(k)$. Vse vrednosti ρ so manjše od 2, razen v primeru $k = 3, 6, 15$.

k	ℓ	$t(x)$, $r(x)$, $q(x)$	ρ
15	120	$t(x) = x^{28}+x^{24}-x^{16}-x^{12}-x^8+1$ $r(x) = \Phi_{120}(x)$ $q(x) = (2x^{56}+4x^{52}+x^{50}+2x^{48}+2x^{46}-4x^{44}$ $-6x^{40}-4x^{36}-x^{30}+12x^{28}-2x^{26}+14x^{24}$ $-x^{22}+2x^{20}-10x^{16}-10x^{12}+x^{10}-8x^8$ $+2x^6+x^2+8)/8$	7/4
25	56	$t(x) = -x^2$ $r(x) = \Phi_{56}(x)$ $q(x) = (2(x^2-1)^2+x^{14}(x^2+1)^2(x^{14}+1)^2)/8$	23/12
44	88	$t(x) = -x^2$ $r(x) = \Phi_{88}(x)$ $q(x) = (2(x^2-1)^2+x^{22}(x^2+1)^2(x^{22}+1)^2)/8$	7/4

Tabela 7.7.1: Družine krivulj s $k \in \{15, 28, 44\}$ in $D = 2$.

Dokaz. Uporabili bomo izrek 7.7.1 v obsegu $K = \mathbb{Q}[x]/(\Phi_\ell(x))$, ki je izomorfen obsegu $\mathbb{Q}(\zeta_k, \zeta_8) = \mathbb{Q}(\zeta_{\mathrm{lcm}(k,8)})$. Naj elementa ζ_k in $\sqrt{-2} = \zeta_8+\zeta_8^3$ obsega K ustrezata polinomoma $x^{\ell/k}$ in $x^{\ell/8}+x^{3\ell/8}$. Iščemo tak polinom $y(x)$, ki bo ustrezal elementu $(\zeta_k-1)/\sqrt{-2}$). Polinom $z(x) = (1-x^{\ell/k})(x^{3\ell/8}+x^{\ell/8})/2$ ustreza elementu $(\zeta_k-1)/\sqrt{-2}$. Ker je k večkratnik 3, lahko uporabimo $x^{\ell/3} \equiv x^{\ell/6}-1 \mod \Phi_\ell(x)$, da polinom $z(x)$ reduciramo v polinom $y(x) = (1-x^{\ell(k)}(x^{5\ell/24}+x^{\ell/8}-x^{\ell/24})/2$. Če izberemo $t(x) = x^{\ell/k}+1$ dobimo $q(x)$ kot v konstrukciji 7.7.7. Če je $k \neq 3, 6, 15$, potem je $\frac{\ell}{k}+\frac{5\ell}{24} < \varphi(\ell)$ in polinom $y(x) \mod \Phi_l(x)$ res ustreza elementu $(\zeta_k-1)/\sqrt{-2}$ obsega K. Dokazati moramo le še, da $q(x)$ predstavlja praštevila. Velja, da je $q(1) = 1$ in z računalnikom [24, 49] lahko pokažemo, da je $q(x)$ nerazcepen za vse vključitvene stopnje $k < 1000$, ki so deljive s 3. Za izračun vrednosti ρ uporabimo dejstvo, da je $\deg(q)) = (\frac{2\ell}{k}+\frac{5\ell}{12})$, $\deg(r) = \varphi(k)\ell/(2k)$ če je k liho in $\deg(r) = \varphi(k)\ell/k$, če je k sodo. ■

Konstrukcija 7.7.7 je sicer samo za vključitvene stopnje k deljive s 3, vendar jo lahko uporabimo za vsako pozitivno število k, če izračunamo polinom $y(x)$, ki ustreza elementu $(\zeta_k-1)/\sqrt{-2}$ v obsegu K. Vendar za razliko od konstrukcije 7.7.6, v primerih ko število k ni deljivo s 3, izraz za polinom $q(x)$ postane preveč kompleksen in v nekaterih primerih konstrukcija ne da družine v smislu definicije 7.3.5. V primeru, ko je število $k = 20$, polinom $q(x)$ iz konstrukcije 7.7.7 nikoli ne zavzame celoštevilske vrednosti. Nekaj potencialnih družin za določene vrednosti vključitvene k je v tabeli 7.7.1.

7.7.2 Sporadične družine Brezing-Weng krivulj

Brezing in Weng sta v svojih konstrukcijah uporabila samo ciklotomične polinome $r(x)$. Včasih pa je uporaba neciklotomičnih polinomov $r(x)$, ki definirajo razširitve ciklotomičnih obsegov, bolj učinkovita. Ena od metod za konstrukcijo takih razširitev je izračun ciklotomičnega polinoma $\Phi_\ell(x)$ za nek polinom $u(x)$. Če je $\Phi_\ell(u(x))$ nerazcepen, kar zaradi nerazcepnosti ciklotomičnega polinoma $\Phi_\ell(x)$ ponavadi je, z razširitvijo ne pridobimo ničesar. V tem primeru namreč računamo vrednosti polinomov t, r in q pri $u(x)$. Če pa $\Phi_l(u(x))$ lahko faktoriziramo, pa lahko dobimo določene prednosti.

Galbraith, McKee in Valença [55] so analizirali faktorizacijo $\Phi_k(u(x))$. Dokazali so naslednjo pomembno lemo.

Lema 7.7.8. *[55, Lema 1]. Naj bo $u(x) \in \mathbb{Q}[x]$ polinom stopnje 2 in naj bo φ Eulerjeva funkcija. Polinom $\Phi_k(u(x))$ ima nerazcepne faktorje stopnje $\varphi(k)$ natanko tedaj, ko ima enačba*

$$u(x) = \zeta_k$$

rešitev v $\mathbb{Q}(\zeta_k)$. Sicer je polinom $\Phi(u(x))$ nerazcepen nad $\mathbb{Q}$ stopnje $2\varphi(k)$.

Dokaz. Naj bo θ poljuben koren $\Phi_k(u(x)) = 0$. Potem je $u(\theta) = \zeta_k$ primitivni k-ti koren enote in $\zeta_k \in \mathbb{Q}(\theta)$. Posledično ima θ stopnjo, ki je večkratnik $\varphi(k)$ nad $\mathbb{Q}$. Še več, θ ima stopnjo $\varphi(k)$ natanko tedaj, ko je θ element razširjenega obsega $\mathbb{Q}(\zeta_k)$. To se zgodi natanko tedaj, ko ima enačba $u(x) = \zeta_k$ rešitev v $\mathbb{Q}(\zeta_k)$, kar pa se zgodi natanko tedaj, ko ima enačba $u(x) = \zeta_k$ rešitev v $\mathbb{Q}(\zeta_k)$. Sicer ima θ stopnjo enako $2\varphi(k)$. ■

Galbraith, McKee in Valença so v svoji analizi pokazali naslednje:

- Za $\ell = 8$ ni nobenega polinoma $u(x)$ stopnje 2, da bi se $\Phi_\ell(u(x))$ faktoriziral.
- Za $\ell = 5$ in $\ell = 10$ obstaja enorazsežna družina polinomov $u(x)$ stopnje 2, ki je parametrizirana z racionalnimi točkami eliptične krivulje nad $\mathbb{Q}$ ranga 1. Ker pa po izreku A.2.39 velja $\mathbb{Q}(\zeta_5) = \mathbb{Q}(\zeta_{10})$ in obseg nima kvadratnega imaginarnega podobsega, ne pričakujemo, da bi našli $\sqrt{-D}$ v katerikoli razširitvi $\mathbb{Q}(\zeta_5)$.
- Za $\ell = 12$ pa obstajata dva polinoma $u(x)$ stopnje 2, za katere je $\Phi_{12}(u(x))$ razcepen.

Barreto in Naehrig sta konstruirala parjenjem prijazno krivuljo praštevilskega reda z uporabo ene izmed teh faktorizacij [11].

Konstrukcija 7.7.9. *Naj bo $k = 12$ in $D = 3$. Definirajmo:*

$$\begin{aligned} r(x) &= 36x^4 + 36x^3 + 18x^2 + 6x + 1, \\ t(x) &= 6x^2 + 1, \\ q(x) &= 36x^4 + 36x^3 + 24x^2 + 6x + 1. \end{aligned}$$

Trojka (t, r, q) parametrizira polno družino krivulj z vključitveno stopnjo k in diskriminanto $D = 3$ glede na definicijo 7.3.5. Vrednost ρ te družine je enaka 1.

Dokaz. Naj bo $u(x) = 6x^2$ in $r(x)$ polinom iz konstrukcije 7.7.9. Potem velja $\Phi_{12}(u(x)) = r(x)r(-x)$, kar lahko preverimo s pomočjo izračunanega polinoma $\Phi_{12}(x)$ na strani 155. Izberimo obseg $K = \mathbb{Q}[x]/(r(x))$. Naj element ζ_{12} obsega K ustreza polinomu $6x^2$. Element $\zeta_{12} + 1$ ustreza polinomu $t(x)$ v v konstrukciji 7.7.9. Z uporabo enakosti $\sqrt{-3} = 2\zeta_{12}^2 - 1$ izračunamo $y(x) = 6x^2 + 4x + 1$. Po izreku 7.7.1 dobimo polinom $q(x)$ v konstrukciji 7.7.9. Tak izračunani polinom $q(x)$ predstavlja praštevilo, vrednost ρ pa izračunamo po (7.13). ■

Opomba: Ker imata polinoma $q(x)$ in $r(x)$ v zgornji konstrukciji enako stopnjo in vodilna koeficienta, $r(x)$ predstavlja dejansko število točk na eliptični krivulji, ki jo želimo konstruirati. Če sta $q(x)$ in $r(x)$ obe praštevili za neko vrednost x, potem bo taka krivulja imela praštevilski red. Krivulje z $D = 3$ imajo ovoj stopnje 6 [137] in ker je k deljiv s

6, lahko te ovoje uporabimo za preslikavo točk iz $E(\mathbb{F}_{p^{12}})$ v $E(\mathbb{F}_{p^2})$, kar omogoča hitrejše operacije. To sta verjetno tudi glavna razloga, da je ta krivulja implementirana v kar nekaj knjižnicah [160, 159]. Primeri krivulj generiranih s to konstrukcijo so v dodatku B.4.

Barreto in Naehrig sta svojo konstrukcijo predstavila kot MNT družino krivulj, v kateri je desna stran enačbe kompleksnega množenja produkt konstante in popolno kvadratnega polinoma (ang, perfect square polynom). To konstrukcijo lahko razširimo tudi na druge polinome $u(x)$ stopnje 3, za katere se ciklotomični polinom $\Phi_{12}(u(x))$ faktorizira, kar je razvidno v naslednji konstrukciji.

Konstrukcija 7.7.10. *Naj bo $k = 4$ in $D = 3$. Definirajmo:*

$$\begin{aligned} t(x) &= -4x^3, \\ r(x) &= 4x^4 + 4x^3 + 2x^2 + 2x + 1, \\ q(x) &= (16x^6 + 8x^4 + 4x^3 + 4x^2 + 4x + 1)/3. \end{aligned}$$

Trojka (t, r, q) parametrizira polno družino krivulj z vključitveno stopnjo $k = 4$ in diskriminanto $D = 3$ glede na definicijo 7.3.5. Vrednost ρ te družine je 3/2..

Dokaz. Naj bo $u(x) = 2x^2$ in $r(x)$ polinom iz konstrukcije 7.7.10. Potem je $\Phi_{12}(u(x)) = r(x)r(-x)$. Izberimo obseg $K = \mathbb{Q}[x]/(r(x))$. Tako izbrani obseg vsebuje element ζ_4, kateremu naj ustreza polinom $u(x)^3 \equiv -4x^3 - 1 \pmod{r(x)}$. Posledično elementu $\zeta_4 + 1$ ustreza polinom $t(x)$ v konstrukciji 7.7.10. Naj elementu $\sqrt{-3}$ ustreza polinom $8x^3 + 4x^2 + 4x + 3$. Po izreku 7.7.1 konstruiramo polinoma $y(x) = (4x^3 + 4x + 2)/3$ in polinom $q(x)$ v konstrukciji 7.7.10. Ker je $q(x)$ nerazcepen in sta $q(-1) = 7$ in $q(2) = 403$ med seboj tuji si števili, polinom $q(x)$ predstavlja praštevila. Vrednost ρ izračunamo po (7.13). ■

Obstajajo še druge faktorizacije ciklotomičnih polinomov $\Phi_k(u(x))$ za različne vrednosti k in stopnje polinomov $u(x)$. Naslednja konstrukcija je za $k = 8$ v [49], najdemo pa jo tudi v [144].

Konstrukcija 7.7.11. *Naj bo $k = 8$ in $D = 1$. Definirajmo:*

$$\begin{aligned} t(x) &= -9x^3 - 3x^2 - 2x, \\ r(x) &= 9x^4 + 12x^3 + 8x^2 + 4x + 1, \\ q(x) &= (81x^6 + 54x^5 + 45x^4 + 12x^3 + 13x^2 + 6x + 1)/4. \end{aligned}$$

Trojka (t, r, q) parametrizira polno družino krivulj z vključitveno stopnjo $k = 8$ in diskriminanto $D = 1$ glede na definicijo 7.3.5. Vrednost ρ te družine je 3/2.

Dokaz. Naj bo $u(x) = 9x^3+3x^2+2x+1$ in $r(x)$ polinom iz konstrukcije 7.7.10. Potem ima ciklotomični polinom $\Phi_8(u(x))$ nerazcepen faktor $r(x) = 9x^4+12x^3+8x^2+4x+1$. Izberimo obseg $K = \mathbb{Q}[x]/(r(x))$. Tako izbrani obseg vsebuje element ζ_8, kateremu naj ustreza polinom $-u(x)$. Elementu $\sqrt{-1} = \zeta_8^2$ obsega K naj ustreza polinom $-18x^3-15x^2-10x-4$ mod $r(x)$. Iz tega zdaj lahko izračunamo polinom $t(x)$ v konstrukciji 7.7.11 in polinom $y(x) = -3x-1$. Z uporabo izreka 7.7.1 dobimo polinom $q(x)$, ki je enak kot v konstrukciji 7.7.11. Ker je $q(x)$ nerazcepen in $q(1) = 53$ ter $q(-1) = 17$, kar sta različni praštevili, polinom $q(x)$ predstavlja praštevila. Vrednost ρ izračunamo po (7.13). ■

Opomba: Vrednost ρ te družine je slabša kot 5/4 v konstrukciji 7.7.6, vendar pa imajo krivulje z $D = 1$ ovoj stopnje 4 [137] in ker $4 \mid k$, lahko uporabimo ta ovoj za preslikavo točk na krivulji $P \in E(\mathbb{F}_{q^8})$ v obseg $\mathbb{F}_{q^2}$, kar omogoča hitrejše operacije.

Za vključitveno stopnjo $k = 8$ sta Tanaka in Nakamula [145] podala dodatno konstrukcijo, ki ima to lastnost, da sta $r(x)$ in $q(x)$ praštevili za neskončno mnogo celoštevilskih vrednosti x. Primeri krivulj generiranih s to konstrukcijo so v B.5.

Konstrukcija 7.7.12. *Naj bo $k = 8$ in $D = 1$. Definirajmo:*

$$\begin{aligned} t(x) &= -82x^3 - 108x^2 - 54x - 8, \\ r(x) &= -82x^4 + 108x^3 + 54x^2 + 12x + 1, \\ q(x) &= 379906x^6 + 799008x^5 + 705346x^4 + \\ &\quad 33361x^3 + 88945x^2 + 12636x + 745. \end{aligned}$$

Trojka (t, r, q) parametrizira polno družino krivulj z vključitveno stopnjo $k = 8$ in diskriminanto $D = 1$ glede na definicijo 7.3.5. Vrednost ρ te družine je 3/2.

Dokaz. Naj bo $u(x) = 82x^3 + 108x^2 + 54x + 9$. Potem ima ciklotomični polinom $\Phi_8(u(x))$ nerazcepen faktor $r(x) = -82x^4 + 108x^3 + 54x^2 + 12x + 1$. Izberimo obseg $K = \mathbb{Q}[x]/(r(x))$. Tako izbran obseg vsebuje elementa ζ_8 in $\sqrt{-1} = \zeta_8^2$, ki jima ustrezata polinoma $u(x)$ in $12966x^3 + 4793x^2 - 13x - 1 \mod r(x)$. Iz tega zdaj lahko izračunamo polinom $t(x)$ v konstrukciji 7.7.12 in polinom $y(x) = -174x^3 - 66x^2 - 12x + 310$. Z uporabo izreka 7.7.1 dobimo $q(x)$, ki je enak kot v konstrukciji 7.7.12. Ker sta vrednosti $q(104) = 490506332802458249$ in $r(104) = 9714910817$ praštevili in ker sta $q(x)$ in $r(x)$ nerazcepna nas $\mathbb{Q}$, polinom $q(x)$ predstavlja praštevila. Vrednost ρ izračunamo po (7.13). ■

Kachisa, Schaefer in Scott [71] so na podlagi [70] podali strategijo za konstrukcijo neciklotomičnih polinomov, ki definirajo ciklotomične obsege. Njihova strategija temelji na izbiri elementa $\beta \in \mathbb{Q}(\zeta_\ell)$, ki ga je mogoče zapisati kot linearno celoštevilsko kombinacijo potenc z majhnimi koeficienti. Minimalni polinom tako izbranega elementa β je polinom $r(x)$ v izreku 7.7.1. Ker večina elementov obsega $\mathbb{Q}(\zeta_\ell)$ ne leži v pravem podobsegu, je v večini primerov $\mathbb{Q}[x]/(r(x)) \cong \mathbb{Q}(\zeta_\ell)$ [93, poglavje 4]. Naslednjih 5 konstrukcija uporablja to strategijo.

Konstrukcija 7.7.13. *Naj bo $k = \ell = 16$ in $D = 1$. Definirajmo:*

$$\begin{aligned} t(x) &= (2x^5 + 41x + 35)/35, \\ r(x) &= x^8 + 48x^4 + 625, \\ q(x) &= (x^{10} + 2x^9 + 5x^8 + 48x^6 + 152x^5 + 240x^4 + 625x^2 + 2398x + 3125)/980. \end{aligned}$$

Trojka (t, r, q) parametrizira polno družino krivulj z vključitveno stopnjo $k = 16$ in diskriminanto $D = 1$ glede na definicijo 7.3.5. Vrednost ρ te družine je 5/4.

Dokaz. Izberimo element $\beta = -2\zeta_{16}^5 + \zeta_{16} \in \mathbb{Q}(\zeta_{16})$. Njegov minimalni polinom je polinom $r(x)$ v konstrukciji 7.7.13. Naj bo $K = \mathbb{Q}(\zeta_{16}) \cong \mathbb{Q}[x]/(r(x))$ in naj elementoma ζ_{16} in $\sqrt{-1}$ ustrezata polinoma $(2x^5 + 41x)/35$ in $(x^4 + 24)/7$ zaporedoma. Element $\zeta_{16} + 1$ potem ustreza polinomu $t(x)$ v konstrukciji 7.7.13 in po izreku 7.12 dobimo polinom $y(x) = -(x^5 + 5x^4 + 38x + 120)/35$ in polinom $q(x)$ v konstrukciji 7.7.13. Polinom $q(x)$ je nerazcepen in $q(x)$ ter $t(x)$ imata celoštevilski vrednosti za $x \in \mathbb{Z}$ natanko tedaj, ko

je $x \equiv 25 \pmod{70}$ ali $x \equiv 45 \pmod{70}$. Ker je $\gcd(\{q(\pm 25 + 70n) : \ n \in \mathbb{Z}\}) = 1$ (to dokažemo z računalnikom in indukcijo po n), $q(x)$ predstavlja praštevila. Vrednost ρ izračunamo po (7.13). ■

Konstrukcija 7.7.14. *Naj bo $k = \ell = 18$ in $D = 3$. Definirajmo:*

$$\begin{aligned} t(x) &= (x^4 + 16x + 7)/7, \\ r(x) &= x^6 + 37x^3 + 343, \\ q(x) &= (x^8 + 5x^7 + 7x^6 + 37x^5 + 188x^4 + 259x^3 + 343x^2 + 1763x + 2401)/21. \end{aligned}$$

Trojka (t, r, q) parametrizira polno družino krivulj z vključitveno stopnjo $k = 18$ in diskriminanto $D = 3$ glede na definicijo 7.3.5. Vrednost ρ te družine je $4/3$.

Dokaz. Izberimo element $\beta = -3\zeta_{18}^5 + \zeta_{18}^2 \in \mathbb{Q}(\zeta_{18})$. Njegov minimalni polinom je polinom $r(x)$ v konstrukciji 7.7.14. Naj bo $K = \mathbb{Q}(\zeta_{18}) \cong \mathbb{Q}[x]/(r(x))$ in naj elementoma ζ_{18} in $\sqrt{-3}$ ustrezata polinoma $(x^4 + 16x)/7$ in $x^3 + 18$ zaporedoma. Elementu $\zeta_{18} + 1$ potem ustreza polinom $t(x)$ v konstrukciji 7.7.14 in po izreku 7.7.1 dobimo polinom $y(x) = -(3x^4 + 15x^3 + 55x + 270)/21$ in polinom $q(x)$ v konstrukciji 7.7.14. Polinom $q(x)$ je nerazcepen. Za $x \equiv 14 \pmod{42}$ ima polinom $t(x)$ celoštevilske vrednosti, polinom $q(x)$ pa ima za take x praštevilske vrednosti. Vrednost ρ izračunamo po (7.13). ■

Konstrukcija 7.7.15. *Naj bo $k = \ell = 32$ in $D = 1$. Definirajmo:*

$$\begin{aligned} t(x) &= (-2x^9 - 56403x + 3107)/3107, \\ r(x) &= x^{16} + 57120x^8 + 815730721, \\ q(x) &= (x^{18} + 6x^{17} + 13x^{16} + 57120x^{10} - 344632x^9 + \\ &\quad 742560x^8 + 815730721x^2 - 4948305594x + 10604499373)/2970292 \end{aligned}$$

Trojka (t, r, q) parametrizira polno družino krivulj z vključitveno stopnjo $k = 32$ in diskriminanto $D = 1$ glede na definicijo 7.3.5. Vrednost ρ te družine je $9/8$.

Dokaz. Izberimo element $\beta = -3\zeta_{32} + 2\zeta_{32}^9 \in \mathbb{Q}(\zeta_{32})$. Njegov minimalni polinom je polinom $r(x)$ v konstrukciji 7.7.15. Naj bo $K = \mathbb{Q}(\zeta_{32}) \cong \mathbb{Q}[x]/(r(x))$ in naj elementoma ζ_{32} in $\sqrt{-1}$ ustrezata polinoma $(-2x^9 - 56403x)/3107$ in $(x^8 + 28560)/239$ zaporedoma. Elementu $\zeta_{32} + 1$ ustreza polinom $t(x)$ v konstrukciji 7.7.15 in po izreku 7.7.1 dobimo polinom $y(x) = (-3x^9 + 13x^8 - 86158x + 371280)/3107$ in polinom $q(x)$ v konstrukciji 7.7.15. Polinom $q(x)$ je nerazcepen. Za $x \equiv \pm 325 \pmod{6214}$ ima $t(x)$ celoštevilske vrednosti, polinom $q(x)$ pa ima za take x praštevilske vrednosti. Vrednost ρ izračunamo po (7.13). ■

Konstrukcija 7.7.16. *Naj bo $k = \ell = 36$ in $D = 3$. Definirajmo:*

$$\begin{aligned} t(x) &= (2x^7 + 757x + 259)/259, \\ r(x) &= x^{12} + 683x^6 + 117649, \\ q(x) &= (x^{14} - 4x^{13} + 683x^8 - 25105x^7 + 4781x^6 + \\ &\quad 117649x^2 - 386569x + 823543)/28749 \end{aligned}$$

Trojka (t, r, q) parametrizira polno družino krivulj z vključitveno stopnjo $k = 36$ in diskriminanto $D = 3$ glede na definicijo 7.3.5. Vrednost ρ te družine je $7/6$.

Dokaz. Izberimo element $\beta = 2\zeta_{36} + 2\zeta_{36}^7 \in \mathbb{Q}(\zeta_{36})$. Njegov minimalni polinom je polinom $r(x)$ v konstrukciji 7.7.16. Naj bo $K = \mathbb{Q}(\zeta_{36}) \cong \mathbb{Q}[x]/(r(x))$ in naj elementoma ζ_{36} in $\sqrt{-3}$ ustrezata polinoma $(2x^7 + 757x)/259$ $(x^6 + 323)/37$ zaporedoma. Elementu $\zeta_{36} + 1$ ustreza polinom $t(x)$ v konstrukciji 7.7.16 in po izreku 7.7.1 dobimo polinom $y(x) = (-x^7 + 7x^6 - 249x + 2261)/777$ in polinom $q(x)$ v konstrukciji 7.7.16. Polinom $q(x)$ je nerazcepen. Za $x \equiv 287 \pmod{777}$ ima $t(x)$ celoštevilske vrednosti, $q(x)$ pa ima za take x praštevilske vrednosti. Vrednost ρ izračunamo po (7.13). ■

Konstrukcija 7.7.17. *Naj bo $k = \ell = 40$ in $D = 1$. Definirajmo:*

$$\begin{aligned} t(x) &= (2x^{11} + 6469x + 1185)/1185, \\ r(x) &= x^{16} + 8x^{14} + 39x^{12} + 112x^{10} - 79x^8 + 2800x^6 + \\ &\quad 24375x^4 + 125000x^2 + 390625, \\ q(x) &= (x^{22} - 2x^{21} + 5x^{20} + 6232x^{12} - 10568x^{11} + 31160x^{10} + \\ &\quad 9765625x^2 - 13398638x + 48828125)/1123380. \end{aligned}$$

Trojka (t, r, q) parametrizira polno družino krivulj z vključitveno stopnjo $k = 40$ in diskriminanto $D = 1$ glede na definicijo 7.3.5. Vrednost ρ te družine je $11/8$.

Dokaz. Izberimo element $\beta = 2\zeta_{40} + 2\zeta_{40}^{11} \in \mathbb{Q}(\zeta_{40})$. Njegov minimalni polinom je polinom $r(x)$ v konstrukciji 7.7.17. Naj bo $K = \mathbb{Q}(\zeta_{40}) \cong \mathbb{Q}[x]/(r(x))$ in naj elementoma ζ_{40} in $\sqrt{-1}$ ustrezata polinoma $(2x^{11} + 6469x)/1185$ in $(x^{10} + 3116)/237$ zaporedoma. Elementu ζ_{40} ustreza polinom $t(x)$ v konstrukciji 7.7.17 in po izreku 7.7.1 dobimo polinom $y(x) = (-x^{11} + 5x^{10} - 2642x + 15580)/1185$ in polinom $q(x)$ v konstrukciji 7.7.17. Polinom $q(x)$ je nerazcepen. Za $x \equiv \pm 20 \pmod{1185}$ ima $t(x)$ celoštevilske vrednosti, polinom $q(x)$ pa ima za take x praštevilske vrednosti. Vrednost ρ izračunamo po (7.13). ■

7.7.3 Scott-Barreto družine

Za Scott-Barret strategijo [136] bomo ponovno vzeli obseg K kot razširitev ciklotomičnih obsegov, le da tokrat ne bomo predpostavili $\sqrt{-D} \in K$. Če izberemo $t(x)$ kot poljuben polinom in $r(x)$ kot nerazcepen faktor polinoma $\Phi_k(t(x) - 1)$, potem je obseg $\mathbb{Q}[x]/(r(x))$ razširitev ciklotomičnega obsega. Nato poiščemo tak polinom $h(x)$, da ima desna stran enačbe kompleksnega množenja

$$Dy^2 = 4h(x)r(x) - (t(x) - 2)^2. \tag{7.15}$$

obliko produkta linearnega faktorja in popolno kvadratnega polinoma. Ko tak $h(x)$ najdemo, lahko naredimo x kot linearno funkcijo spremenljivke Dz^2, ki naredi desno stran enačbe (7.15) oblike produkta D in kvadratnega polinoma spremenljivke z.

Konstrukcija 7.7.18. *Naj bo $k = 6$. Definirajmo:*

$$\begin{aligned} t(x) &= -4x^2 + 4x + 2, \\ r(x) &= 16x^4 - 32x^3 + 12x^3 + 4x + 1, \\ q(x) &= 4x^5 - 8x^4 + 3x^3 - 3x^2 + \tfrac{17}{4}x + 1. \end{aligned}$$

Naj bo $D \in \mathbb{N}$ prosto kvadratov, ki ne deli produkt $2 \cdot 3 \cdot 5 \cdot 911$. Potem trojka $t(Dz^2), r(Dz^2), q(Dz^2))$ parametrizira polno družino krivulj s stopnjo vključitve $k = 6$ in diskriminanto D. Vrednost ρ te družine je $5/4$.

Dokaz. Za polinom $r(x)$ v konstrukciji 7.7.18 velja $r(x) = \Phi_6(t(x)-1)$. Izberimo $h(x) = x/4$, ki nam da $q(x) = h(x)r(x) + t(x) - 1$. Če uporabimo novo spremenljivko z, tako da velja $x = Dz^2$, se enačba kompleksnega množenja (7.15) prevede v

$$Dy^2 = x(4x^2 - 6x + 1)^2 = Dz^2(4D^2z^4 - 6Dz^2 + 1)^2.$$

Ker sta polinoma $4q(x)$ in $r(x)$ nerazcepna v $\mathbb{Z}[x]$, iz trditve A.3.4 sledi, da je $r(Dz^2)$ nerazcepen, če D ne deli $16 \cdot \mathrm{Disc}(r(x)) = 2^{20} \cdot 3^3$ (definicija diskriminante polinoma Disc je v dodatku A.3.2). Podobno je $q(Dz^2)$ nerazcepen, če D ne deli $64 \cdot \mathrm{Disc}(4q(x)) = 2^{22} \cdot 5^3 \cdot 911$. Ker je $q(0) = 1$ za poljuben $D \in \mathbb{N}$ prost kvadratov, sledi, da $q(Dz^2)$ predstavlja praštevilo če le $D \nmid 2 \cdot 5 \cdot 911$. ■

Naslednjo konstrukcijo Koblitza in Menezesa [81] lahko gledamo kot primer Scott-Barreto konstrukcije, pri kateri je polinom $h(x) = D\ell^2$ za poljuben D prost kvadratov in sodi $\ell \in \mathbb{Z}$.

Konstrukcija 7.7.19. *Naj bo ℓ sodo celo število in naj bo $D \in \mathbb{N}$ prosto kvadratov. Definirajmo:*

$$\begin{aligned} t(x) &= 2, \\ r(x) &= x, \\ q(x) &= D\ell^2x^2 + 1. \end{aligned}$$

Trojka (t, r, q) parametrizira polno družino krivulj z vključitveno stopnjo $k = 1$ in diskriminanto D glede na definicijo 7.3.5. Vrednost ρ te družine je enaka 2.

Dokaz. Polinom $r(x)$ je nerazcepen, polinom $q(x)$ pa predstavlja praštevila za vsaki pozitivni števili ℓ in D. Nadalje, polinom $r(x)$ deli $q(x) + 1 - t(x) = D\ell^2x^2$ in $r(x)$ deli ciklotomični polinom $\Phi_1(t(x) - 1) = 0$. ■

Koblitz in Menezes sta podala dva primera eliptične krivulje za zgornjo konstrukcijo [81] in sicer:

$$\begin{aligned} y^2 = x^3 - x, &\quad \text{če } \ell x \equiv 0 \pmod 4, \\ y^2 = x^3 - 4x, &\quad \text{če } \ell x \equiv 2 \pmod 4. \end{aligned}$$

Zgornja konstrukcija generira eliptično krivuljo z vključitveno stopnjo $k = 1$ in z eno samo ciklično podgrupo reda r primerno za parjenja. Čeprav je splošno prepričanje, da mora biti $E(\mathbb{F}_q)[r]$ izomorfna $(\mathbb{Z}/r\mathbb{Z})^2$, da je zagotovljeno netrivialno Tate-Lichtenbaumovo parjenje [68, 69], pa ta pogoj ni potreben [127]. Prepričanje pride iz dejstva, da so na krivulji z vključitveno stopnjo $k > 1$, vse r-torzijske točke definirane nad $\mathbb{F}_{q^k}$ [5]. V praksi pa imajo krivulje konstruirane z metodo kompleksnega množenja, ki imajo vključitveno stopnjo $k = 1$, r-torzijske točke definirane nad osnovnim obsegom. Velja namreč naslednja trditev.

Trditev 7.7.20. *[49, Trditev 6.18]. Naj bo $E/\mathbb{F}_q$ navadna eliptična krivulja, ki ima vključitveno stopnjo $k = 1$ glede na praštevilo r in diskriminanto kompleksnega množenja D. Če $r \nmid 2CD$, kjer je C prevodnik $[\mathcal{O} : \mathrm{End}(E)]$ in $\mathcal{O}$ kolobar celih števil v $\mathbb{Q}(\sqrt{-D})$, potem velja $E[r] \subset E(\mathbb{F}_q)$.* ■

7.8 Družine z variabilno diskriminanto

V konstrukcijah, ki smo jih predstavili v prejšnjih razdelkih, smo diskriminanto D vedno fiksirali in nato konstruirali eliptično krivuljo. V tem razdelku si bomo ogledali dva primera, ko je diskriminanta D enačbe kompleksnega množenja variabilna. V prvem primeru bomo vzeli vrednost diskriminante D kot parameter pri generiranju krivulje in ne že ob konstrukciji polinomov (t, r, q). V drugem primeru pa bomo sledili definiciji polne družine z variabilno diskriminanto podane v 7.3.5.

7.8.1 Ciklotomične družine

Izrek 7.8.1. *Predpostavimo, da trojka sodih polinomov (t, r, q) parametrizira polno potencialno družino eliptičnih krivulj z vključitveno stopnjo k in diskriminanto D. Naj bo $y(x)$ polinom, kot v definiciji 7.3.5, ki je lih. Definirajmo polinome t', r', q' in y' kot:*

$$t(x) = t'(x^2), \quad r(x) = r'(x^2), \quad q(x) = q'(x^2), \quad y(x) = y'(x^2).$$

Izberimo tak $\alpha \in \mathbb{N}$, da velja:

1. *Produkt αD je prost kvadratov;*
2. *Polinom $r'(\alpha x^2)$ je nerazcepen;*
3. *Polinom $y'(\alpha x^2)$ ima celoštevilsko vrednost za neko celo število x.*

Potem trojka $(t'(\alpha x^2), r'(\alpha x^2), q'(\alpha x^2))$ parametrizira polno potencialno družino eliptičnih krivulj z vključitveno stopnjo k in diskriminanto αD. Vrednost ρ take družine je enaka vrednosti $\rho(t, r, q)$ definirane v (7.7).

Dokaz. Za vsak α, ki zadostuje pogojem izreka 7.8.1, moramo preveriti pogoje (b) - (e) točke 1. definicije 7.3.5 (potencialna družina) za trojko $(t'(\alpha x^2), r'(\alpha x^2), q'(\alpha x^2))$. Če je $r'(\alpha x^2)$ nerazcepen, potem pogoj (b) točke 1. za polinom $r'(\alpha x^2)$ velja iz pogoja za polinom $r(x)$. Pogoja (c) in (d) točke 1. definicije 7.3.5 sta enakosti za r, t in q in veljata tudi, če izračunamo polinome v $\sqrt{\alpha}x$. Izračun enačbe kompleksnega množenja (7.12) pri $\sqrt{\alpha}x$ nam da naslednjo enakost:

$$4q'(\alpha x^2) - t'(\alpha x^2)^2 = D \cdot \alpha x^2 \cdot y'(\alpha x^2)^2.$$

Ker je $y'(\alpha x^2) \in \mathbb{Z}$ za nek x, velja enako za neskončno mnogo vrednosti x in s tem je dokazan tudi pogoj (e) točke 1. definicije 7.3.5. Za vrednost ρ družine pa velja naslednje:

$$\rho(t'(\alpha x^2), r'(\alpha x^2), q'(\alpha x^2)) = \frac{2 \deg q'}{2 \deg r'} = \frac{2 \deg q}{2 \deg r} = \rho(t, r, q).$$

■

Iz izreka 7.8.1 sledi, da če so polinomi $t(x), r(x), q(x)$ sodi ($t(x) = t(-x)$,$r(x) = r(-x)$ in $q(x) = q(-x)$) in je polinom $z(x) \mod r(x)$, ki ustreza elementu $\sqrt{-D}$, lih polinom ($z(-x) = -z(x)$), potem nam zamenjava spremenljivk $x^2 \mapsto \alpha x^2$ lahko da potencialno družino krivulj z diskriminanto αD. Najtežji del pri generiranju take družine je v zagotavljanju, da $q'(\alpha x^2)$ predstavlja praštevila, saj pogosto dobimo $\gcd\{q(x) : x, q(x) \in \mathbb{Z}\} > 1$. Prva uporaba izreka 7.8.1 bo v naslednji konstrukciji, ki je izboljšava konstrukcije 7.7.2 za določene lihe vrednosti vključitvene stopnje k.

Konstrukcija 7.8.2. *Naj bo k liho naravno število. Definirajmo:*

$$\begin{aligned} t(x) &= 1+(-1)^{(k+1)/2}x^{k+1}, \\ r(x) &= \Phi_{4k}(x), \\ q(x) &= \left(x^{2k+2}+x^{2k}+4(-1)^{(k+1)/2}x^{k+1}+x^2+1\right)/4. \end{aligned} \tag{7.16}$$

Trojka (t,r,q) parametrizira polno potencialno družino eliptičnih krivulj glede na definicijo 7.3.5 z vključitveno stopnjo k in diskriminanto $D=1$. Vrednost ρ te družine je $(k+1)/\varphi(k)$.

Dokaz. Uporabimo izrek 7.7.1 v obsegu $K=\mathbb{Q}[x]/(r(x)) \cong \mathbb{Q}(\zeta_k,\sqrt{-1})$. Naj elementoma ζ_k in $\sqrt{-1}$ obsega K ustrezata polinoma $(-1)^{(k+1)/2}x^k+1$ in x^k zaporedoma. Potem elementu $(\zeta_k-1)/\sqrt{-1}$ ustreza polinom $(1-(-1)^{(k+1)/2}x^{k+1})x^k \equiv (-1)^{(k+1)/2}x+x^k$ mod $r(x)$ in za $y(x)$ izberemo $y(x)=(-1)^{(k+1)/2}x+x^k$. Zdaj lahko izračunamo

$$q(x)=\frac{1}{4}\left(\left((-1)^{(k+1)/2}x^{k+1}+1\right)^2+\left((-1)^{(k+1)/2}x+x^k\right)^2\right),$$

ki se poenostavi v $q(x)$ v (7.16). Iz dejstva $\deg q = 2k+2$ in $\deg r = 2\varphi(k)$ sledi $\rho=(k+1)/\varphi(k)$. ■

Konstrukcija 7.8.3. *Naj bo k liho naravno število. Definirajmo:*

$$\begin{aligned} t(x) &= 1-(-1)^{(k+1)/2}x^{k+1}, \\ r(x) &= \Phi_{4k}(x), \\ q(x) &= (x^{2k+2}+x^{2k}-4(-1)^{(k+1)/2}x^{k+1}+x^2+1)/4. \end{aligned}$$

Trojka (t,r,q) parametrizira polno potencialno družino krivulj z vključitveno stopnjo $2k$ in diskriminanto $D=1$. Vrednost ρ te družine je enaka $(k+1)/\varphi(k)$.

Dokaz. Izberimo obseg $K=\mathbb{Q}[x]/(r(x)) \cong \mathbb{Q}(\zeta_{2k},\sqrt{-1})$. Naj elementoma ζ_{2k} in $\sqrt{-1}$ obsega K ustrezata polinoma $-(-1)^{(k+1)/2}x^{k+1}$ in x^k zaporedoma. Ostalo je enako kot v dokazu konstrukcije 7.8.2. ■

Opomba: S kombinacijo substitucije $x^2 \mapsto \alpha x^2$ iz izreka 7.8.1 (za nek primeren α) in konstrukcijami 7.7.2, 7.7.3, 7.7.7, 7.8.2 ali 7.8.3 lahko generiramo družino parjenjem prijaznih eliptičnih krivulj z variabilno diskriminanto D za vsak k, ki zadostuje pogoju $\gcd(k,24) \in \{1,2,3,6,12\}$.

Algoritem 7.8.1 Algoritem za generiranje družin krivulj z variabilno diskriminanto

Vhodni podatki: vključitvena stopnja $k \in \mathbb{N}$, za katero velja $\gcd(k, 24) \in \{1, 2, 3, 6, 12\}$, konstrukcije 7.7.2, 7.7.3, 7.7.7, 7.8.2 in 7.8.3.
Rezultat: diskriminanta D in trojka (t', r', q'), ki parametrizira družino krivulj z vključitveno stopnjo k in diskriminanto D.

1. Glede na vrednost k izberi:
   - Konstrukcijo 7.7.2, če je k liho;
   - Konstrukcijo 7.7.3, če je $k \equiv 2 \pmod 4$;
   - Konstrukcijo 7.7.7, če $3 \nmid k$;
   - Konstrukcijo 7.8.2, če $k \equiv 3 \pmod 4$;
   - Konstrukcijo 7.8.3, če $k \equiv 2 \pmod 8$.
2. Uporabi izbrano osnovno konstrukcijo za izračun trojke (t, r, q), ki parametrizira družino eliptičnih krivulj z vključitveno stopnjo k.
3. Naj bodo t', r', q' in y' taki polinomi, da velja:
$$t(x) = t'(x^2), \quad r(x) = r'(x^2), \quad q(x) = q'(x^2), \quad y(x) = y'(x^2).$$
4. Izberi tak $\alpha \in \mathbb{N}$ brez kvadratov, da velja: $\alpha \nmid k \cdot \mathrm{Disc}(q)$, polinom $q'(\alpha x^2)$ predstavlja praštevila in da sta $r'(\alpha x^2)$ in $q'(\alpha x^2)$ nerazcepna. Zadnji pogoj zahteva, da ima α naslednjo obliko:
   - α je liho za konstrukcije 7.7.2, 7.7.3, 7.7.7 in $4 \nmid k$;
   - $\alpha \equiv 1 \pmod 4$ za konstrukcijo 7.7.7 in $4 \mid k$;
   - $\alpha \equiv 3 \pmod 4$ za konstrukcijo 7.8.2 in 7.8.3.
5. Naj bo $D = 2\alpha$ če je uporabljena konstrukcija 7.7.7 in $D = \alpha$ sicer.
6. Vrni trojko (t', r', q') in diskriminanto D.

Rezultat algoritma 7.8.1 je diskriminanta D in trojka $(t'(\alpha x^2), r'(\alpha x^2), q'(\alpha x^2))$, ki parametrizira družino eliptičnih krivulj z vključitveno stopnjo k in diskriminanto D. Pri vrednostih $\alpha \in \mathbb{N}$ in $x \in \mathbb{Z},$, za kateri je $q'(\alpha x^2)$ praštevilo, obstaja eliptična krivulja nad obsegom $\mathbb{F}_{q'(\alpha x^2)}$ s podgrupo reda $r'(\alpha x^2)$ in vključitveno stopnjo k. Če je $D < 10^{12}$, potem enačbo za to krivuljo izračunamo s metode kompleksnega množenja (glej razdelek 4.9). Čeprav lahko Cocks-Pinch metodo po izreku 7.5.1 uporabimo za generiranje eliptičnih krivulj s poljubno diskriminanto kompleksnega množenja D in vključitveno stopnjo k, je vrednost ρ takih krivulj vedno enaka 2. Prednost algoritma 7.8.1 je v tem, da je diskriminanta kompleksnega množenja variabilna in je dobljena vrednost ρ strogo manjša od 2 za mnogo vrednosti vključitvene stopnje k.

7.8.2 Polne družine z variabilno diskriminanto

Drugi primer konstrukcij družin z variabilno diskriminanto sledi točki 5. v definiciji 7.3.5. Te konstrukcije so nove in v originalni taksonomiji [49] niso bile vključene. V nadaljevanju bomo tako predstavili konstrukcije povzete po [89].

Spomnimo se, da smo polno družino z variabilno diskriminanto definirali v definiciji 7.3.5 kot družino krivulj, za katere se enačbo kompleksnega množenja $Dy^2 = 4q(x) - t(x)^2$ da zapisati bodisi kot $f(x) = 4q(x) - t(x)^2$, bodisi kot $f(x)y(x)^2 = 4q(x) - t(x)^2$, kjer je $f(x)$ linearni polinom .

Oglejmo si najprej prvi scenarij. Naslednja trditev nam bo pomagal pri iskanju polinomov $r(x)$.

Trditev 7.8.4. *Naj $(q(x), r(x), t(x))$ predstavljajo družino eliptičnih krivulj z vključitveno stopnjo $k \geq 3$ in naj ima $d(x) = 4q(x) - t(x)^2$ stopnjo enako 1. Potem ima polinom $r(x)$ ničlo θ oblike $a_1(\zeta_k^\ell - 1)^2 + a_0$, kjer sta a_1 in a_0 racionalni števili, $a_1 \neq 0$ in $\ell \in (\mathbb{Z}/k\mathbb{Z})^*$.*

Dokaz. Ker trojka $(q(x), r(x), t(x))$ predstavlja družino krivulj, lahko zaradi pogoja (c) točke 1. v definiciji 7.3.5 polinom $q(x)$ zapišemo v obliki $q(x) = r(x)h(x) + t(x) - 1$. Iz predpostavke v trditvi sledi $d(x) = 4r(x)h(x) - (t(x) - 2)^2$. Naj bo θ ničla polinoma $r(x)$. Zapišimo $d(x)$ v obliki $d(x) = b_0 + b_1 x$, kjer sta $b_0, b_1 \in \mathbb{Q}$. Po izreku 7.7.1 je polinom $r(x)$ faktor ciklotomičnega polinoma $\Phi_k(t(x)-1)$, posledično je $\Phi_k(t(\theta)-1) = 0$ in $t(\theta) = \zeta_k^\ell + 1$ za nek $\ell \in (\mathbb{Z}/k\mathbb{Z})^*$. Velja $b_0 + b_1\theta = d(\theta) = -(\zeta_k^\ell - 1)^2$. Če vzamemo za $a_0 = -b_0/b_1$ in za $a_1 = -1/b_1$, je trditev dokazana. ■

Zaradi zgornje trditve je za konstrukcijo eliptičnih krivulj, za katere je $d(x) = 4q(x) - t(x)^2$ linearen polinom dovolj, če iščemo samo polinome $r(x)$, ki imajo korene oblike $\theta = a_1(\zeta_k^\ell - 1)^2 + a_0$. Ker je $r(x)$ nerazcepen nad $\mathbb{Q}$ in $\theta = \sigma_\ell(a_1(\zeta_k^\ell - 1)^2 + a_0)$ za nek $\sigma_\ell \in \mathrm{Gal}_{\mathbb{Q}(\zeta_k)/\mathbb{Q}}$, je dovolj če gledamo primer $\ell = 1$. Naslednji izrek opiše metodo za generiranje takih krivulj.

Izrek 7.8.5. *Naj bo k naravno število, $\theta = a_1(\zeta_k - 1)^2 + a_0$ element ciklotomičnega obsega $K = \mathbb{Q}(\zeta_k)$, kjer sta $a_0, a_1 \in \mathbb{Q}$, $a_1 \neq 0$, in $r(x) \in \mathbb{Z}[x]$ nerazcepen polinom za katerega velja $r(\theta) = 0$. Izberimo polinom $t(x) \in \mathbb{Q}[x]$, ki ustreza elementu $\zeta_k + 1 \in K$, in definirajmo naslednja polinoma:*

1. $d(x) = (-x + a_0)/a_1 \in \mathbb{Q}[x]$;

2. $q(x) = (t(x)^2 + d(x))/4 \in \mathbb{Q}[x]$.

Če polinoma $q(x)$ in $r(x)$ predstavljata praštevila in je $t(x) \in \mathbb{Z}$ za nek $x \in \mathbb{Z}$, potem trojka $(t(x), r(x), q(x))$ parametrizira družino eliptičnih krivulj v smislu definicije 7.3.5, za katero je $d(x) = 4q(x)^2 - t(x)^2$ linearen polinom.

Dokaz. Najprej bomo dokazali, da je $\mathbb{Q}(\zeta_k)$ izomorfen obsegu $\mathbb{Q}[x]/(r(x))$ za polinom $r(x)$ iz izreka. Oglejmo si Galoisovo grupo razširitve $\mathbb{Q}(\zeta_k)$ nad $\mathbb{Q}$. Za vsak $\sigma_i \in \mathrm{Gal}_{\mathbb{Q}(\zeta_k)/\mathbb{Q}}$, $i \in (\mathbb{Z}/k\mathbb{Z})^*$ velja $\sigma_i(\zeta_k) = \zeta_k^i$ [85]. Ker je $\theta = a_1(\zeta_k - 1)^2 + a_0$ in $(\sigma_i(\zeta_k) - 1)^2 \neq (\sigma_j(\zeta_k) - 1)^2$ za $i \neq j \in (\mathbb{Z}/k\mathbb{Z})^*$, je $\sigma_i(\theta) \neq \sigma_j(\theta)$. Posledično mora imeti polinom $r(x)$ vsaj $\varphi(k)$ korenov in obseg $\mathbb{Q}(\zeta_k)$ je enak $\mathbb{Q}(\theta)$. Slednji pa je izomorfen $\mathbb{Q}[x]/(r(x))$. Zdaj je potrebno dokazati še, da trojka $(q(x), r(x), t(x))$ zadošča pogojema (c) in (d) točke 1. v definiciji 7.3.5. Iz definicije polinoma $t(x)$ v izreku sledi, da polinom $r(x)$ deli $\Phi_k(t(x)-1)$. Poleg tega polinom $x \in \mathbb{Q}[x]$ ustreza elementu $a_1(\zeta_k - 1)^2 + a_0$ v obsegu $\mathbb{Q}(\zeta_k)$, saj je $\theta = a_1(\zeta_k - 1)^2 + a_0$ koren polinoma $r(x)$. Posledično je $x \equiv a_1(t(x) - 2)^2 + a_0 \pmod{r(x)}$ v $\mathbb{Q}[x]/(r(x))$. Polinom x lahko zapišemo v obliki $x = a_1(\zeta_k - 1)^2 + a_0 + h(x)r(x)$ za nek $h(x) \in \mathbb{Q}[x]$. Velja

$$\begin{aligned} q(x) &= (t(x)^2 + d(x))/4 = \left(t(x)^2 - \tfrac{1}{a_1}x + \tfrac{a_0}{a_1}\right)/4 \\ &= \left(t(x)^2 - \tfrac{1}{a_1}\left(a_1(t(x)-2)^2 + a_0 + h(x)r(x)\right) + \tfrac{a_0}{a_1}\right)/4 \\ &= \left(t(x)^2 - (t(x)-2)^2 - \tfrac{h(x)}{a_1}r(x)\right)/4 \\ &= t(x) - 1 - \tilde{h}(x)r(x), \end{aligned}$$

kjer je $\tilde{h}(x) = -h(x)/4a_1$. ■

Naslednja konstrukcija temelji na zgornjem izreku.

Konstrukcija 7.8.6. *Naj bo $k = 5$. Definirajmo*

$$\begin{aligned} t(x) &= (x^3 + x^2 + 19x + 20)/55, \\ r(x) &= x^4 - 3x^2 + 4x^2 - 12x + 41, \\ q(x) &= (x^6 + 2x^5 + 39x^4 + 78x^3 + 401x^2 + 3785x - 5450)/12100. \end{aligned}$$

Če je $x \in \mathbb{Z}$, $x \equiv -3 \pmod{220}$, potem polinom $t(x)$ predstavlja cela števila, polinoma $q(x)$ in $r(x)/275$ pa praštevila. Trojka (t, r, q) parametrizira družino krivulj z vključitveno stopnjo $k = 5$ glede na definicijo 7.3.5. Vrednost ρ te družine je $3/2$.

Po [89, izrek 3.6] ne obstajajo trojke polinomov $(q(x), r(x), t(x))$, ki bi parametrizirale družino krivulj glede na pogoj (7.5) za naslednje vrednosti vključitvene stopnje $k \in \{3, 4, 6, 8, 10, 12, 15, 16, 24, 30, 32, 39, 40, 48\}$. Za te vrednosti k lahko dobimo družine krivulj, če je diskriminanta D oblike $xf(x)^2$. Velja naslednji izrek.

Izrek 7.8.7. *Naj bo k naravno število, ζ_ℓ primitivni ℓ-ti koren enote, kjer $k \mid \ell$, in $\alpha \neq 0$ tak element obsega $K = \mathbb{Q}(\zeta_\ell)$, da je $\mathbb{Q}(\theta) \cong \mathbb{Q}(\zeta_\ell)$ za $\theta = -(\frac{\zeta_k - 1}{\alpha})^2$. Naj bo $r(x) \in \mathbb{Z}[x]$ tak nerazcepen polinom, da je $r(\theta) = 0$ in $\mathbb{Q}[x]/(r(x)) \cong \mathbb{Q}(\zeta_\ell)$. Izberimo polinome $x, t(x), f(x) \in \mathbb{Q}[x]$, ki ustrezajo elementom $-(\frac{\zeta_k - 1}{\alpha})^2$, $\zeta_k + 1$ in α v obsegu $\mathbb{Q}(\zeta_\ell)$. Definirajmo polinom $q(x) = (t(x)^2 + xf(x)^2)/4 \in \mathbb{Q}[x]$. Če polinoma $q(x)$ in $r(x)$ predstavljata praštevila in je $t(x) \in \mathbb{Z}$ za nek $x \in \mathbb{Z}$, potem trojka $(t(x), r(x), q(x))$ parametrizira družino eliptičnih krivulj z vključitveno stopnjo k v smislu definicije 7.3.5, za katero velja $xf(x)^2 = 4q(x)^2 - t(x)^2$.*

Dokaz. Dokazati je potrebno, da trojka $(q(x), r(x), t(x))$ zadošča pogoju (c) točke 1. v definiciji 7.3.5. Opazimo, da je $x \equiv -((t(x)-2)/f(x))^2 \pmod{r(x)}$ v $\mathbb{Q}[x]/(r(x))$. Posledično lahko produkt $xf(x)^2$ zapišemo kot $-(t(x)-2)^2+h(x)r(x)$ za nek $h(x) \in \mathbb{Q}[x]$. Velja

$$\begin{aligned} q(x) &= (t(x)^2 + xf(x)^2)/4 \\ &= (t(x)^2 - (t(x)-2)^2 + h(x)r(x))/4 \\ &= t(x) - 1 + \tilde{h}(x)r(x), \end{aligned}$$

kjer je $\tilde{h}(x) = -\frac{h(x)}{4a_1}$. Ostali koraki so enaki kot v dokazu izreka 7.8.5. ■

Naslednje štiri konstrukcije temeljijo na zgornjem izreku. Pomembne so zato, ker dopolnjujejo originalni seznam priporočenih krivulj v [49], v katerem za vključitvene stopnje $k = 8$, $k = 16$, $k = 20$ in $k = 24$, ni bilo znanih konstrukcij z variabilno diskriminanto.

Konstrukcija 7.8.8. *Naj bo $k = 8$. Definirajmo:*

$$\begin{aligned} \alpha &= 2\zeta_k^3 - \zeta_k^2 - \zeta_k + 2, \\ t(x) &= (3x^3 - x^2 + 99x + 7)/24, \\ r(x) &= x^4 + 34x^2 + 1, \\ q(x) &= (49x^7 + 51x^6 + 3349x^5 + 3415x^4 + 57559x^3 + 57109x^2 + 11187x + 49)/2304. \end{aligned}$$

Če je $x \in \mathbb{Z}$, $x \equiv 7, 11 \pmod{12}$, potem polinom $t(x)$ predstavlja cela števila, polinoma $q(x)$ in $r(x)/6^2$ pa praštevila. Trojka (t, r, q) parametrizira družino krivulj z vključitveno stopnjo $k = 8$ glede na definicijo 7.3.5. Vrednost ρ te družine je $7/4$.

Konstrukcija 7.8.9. *Naj bo $k = 16$. Definirajmo:*

$$\begin{aligned} \alpha &= \zeta_k^4 - 2\zeta_k^3 + \zeta_k^2 - \zeta_k, \\ t(x) &= (-1673x^7 - 131x^6 - 555345x^5 - 43523x^4 - 1104075x^3 \\ &\quad -99081x^2 - 63931x - 337)/15232 \\ r(x) &= x^8 + 332x^6 + 678x^4 + 76x^2 + 1, \\ q(x) &= (117310561x^{15} + 39039455x^{14} + 77892835753x^{13} + 25919226855x^{12} \\ &\quad +13088598379413x^{11} + 4354049399243x^{10} + 52676581062573x^9 \\ &\quad +17249623655107x^8 + 59240325856323x^7 + 18576763413053x^6 \\ &\quad +11456416399483x^5 + 2590174825717x^4 + 621744760071x^3 \\ &\quad +91546735321x^2 + 4130262255x + 113569)/928055296. \end{aligned}$$

Če je $x \in \mathbb{Z}$, $x \equiv 67, 87, 115, 123, 151, 171, 291, 319, 339, 375, 395, 423 \pmod{2^2 \cdot 17 \cdot 7}$, potem polinom $t(x)$ predstavlja cela števila, polinoma $q(x)$ in

$$\tilde{r}(x) = \begin{cases} r(x)/(2^6 \cdot 7^2 \cdot 17), & \text{če je } x \equiv 67, 115, 123, 171, 319, 339, 375, 395, \\ r(x)/(2^6 \cdot 7 \cdot 17^2), & \text{če je } x \equiv 87, 151, 291, 423. \end{cases}$$

pa praštevila. Trojka (t, r, q) parametrizira družino krivulj z vključitveno stopnjo $k = 16$ glede na definicijo 7.3.5. Vrednost ρ te družine je $15/8$.

Konstrukcija 7.8.10. *Naj bo* $k = 20$. *Definirajmo:*

$$\begin{aligned}
\alpha &= -\zeta_k^4 + \zeta_k^3 - \zeta_k^2,\\
t(x) &= (-13x^7 + 93x^6 - 9337x^5 + 66581x^4 - 27071x^3\\
&\quad +40183x^2 - 7131x + 5687)/2624,\\
r(x) &= x^8 + 716x^6 + 486x^4 + 76x^2 + 1,\\
q(x) &= (1879641x^{15} + 1012474x^{14} + 2691199323x^{13} + 1449408872x^{12}\\
&\quad +964796804001x^{11} + 519385215086x^{10} + 1079147931643x^9\\
&\quad +471940038900x^8 + 374562480771x^7 + 136911017622x^6\\
&\quad +35030676649x^5 + 16607083680x^4 - 2271180669x^3 + 1912901570x^2\\
&\quad -322130687x + 129367876)/110166016.
\end{aligned}$$

Če je $x \in \mathbb{Z},\ x \equiv 31, 33, 39, 43, 49, 51 \pmod{2 \cdot 41}$, *potem polinom* $t(x)$ *predstavlja cela števila, polinoma* $q(x)$ *in*

$$\tilde{r}(x) = \begin{cases} r(x)/(2^8 \cdot 41^2) & \text{če je } x \equiv 31, 51,\\ r(x)/(2^8 \cdot 41) & \text{če je } x \equiv 33, 39, 43, 49. \end{cases}$$

pa praštevila. Trojka (t, r, q) *parametrizira družino krivulj z vključitveno stopnjo* $k = 20$ *glede na definicijo 7.3.5. Vrednost* ρ *te družine je* $15/8$.

Konstrukcija 7.8.11. *Naj bo* $k = 24$. *Definirajmo:*

$$\begin{aligned}
\alpha &= 2\zeta_k^7 - 2\zeta_k^6 - 2\zeta_k^5 + 2\zeta_k^3 + 2\zeta_k^2 - \zeta_k - 1,\\
t(x) &= (1720794375x^7 - 1633079475x^6 + 4393526499x^5 - 1303164351x^4\\
&\quad +171245365x^3 + 455207175x^2 + 90977697x - 232405)/1032192,\\
r(x) &= 50625x^8 - 48600x^7 + 129564x^6 - 39528x^5 + 4870x^4 + 13592x^3\\
&\quad +2460x^2 - 88x + 1\\
q(x) &= (27542461768326562500x^{15} - 4736450727426473437 5x^{14}\\
&\quad +15601306111455142125 0x^{13} - 14550829016291451292 5x^{12}\\
&\quad +19275668571492862617 6x^{11} - 56558367114155802783x^{10}\\
&\quad +77952979320344155 8x^9 + 338275836419949954 27x^8\\
&\quad +20595017423351059 72x^7 - 15571543047124718 69x^6\\
&\quad +21140089982485474 38x^5 + 11569749737889116 17x^4\\
&\quad +19671125588253306 4x^3 + 1008248922803059 5x^2\\
&\quad -32616400227974x + 54012084025)/4261681299456.
\end{aligned}$$

Če je $x \in \mathbb{Z},\ x \equiv 31, 44, 55 \pmod{2^2 \cdot 3 \cdot 7}$, *potem* $t(x)$ *predstavlja cela števila,* $q(x)$ *in*

$$\tilde{r}(x) = \begin{cases} r(x)/(2^{16} \cdot 3^2 \cdot 7^2) & \text{če je } x \equiv 31, 43,\\ r(x)/(2^{16} \cdot 3^2) & \text{če je } x \equiv 55. \end{cases}$$

pa praštevila in trojka (t, r, q) *parametrizira družino krivulj z vključitveno stopnjo* $k = 24$ *glede na definicijo 7.3.5,* ρ *vrednost te družine je* $1,875$.

7.9 Implementacija

Pri implementaciji je potrebno upoštevati precej faktorjev. Predstavili bomo samo tiste, ki lahko ključno vplivajo na učinkovitost in s tem tudi na izbiro in konstrukcijo ustrezne krivulje. Ostali faktorji so podrobneje opisani v [116] in [135].

7.9.1 Varnost

Ko izbiramo eliptično krivuljo za implementacijo kriptografske sheme na podlagi parjenj, ponavadi vnaprej fiksiramo želeno velikost b_1 (v bitih) podgrupe praštevilskega reda (podgrupa točk eliptične krivulje) in želeno velikost b_2 (v bitih) končnega obsega, kjer želimo, da je diskretni logaritem težko izračunljiv. Da dosežemo te velikosti, mora veljati $b_2/b_1 = \rho \cdot k$. To razmerje nam dovoljuje uporabo različnih krivulj. V splošnem so zaradi optimizacije aritmetike na eliptični krivulji zaželene krivulje z manjšo vrednostjo ρ. Če vzamemo na primer krivuljo z vključitveno stopnjo $k = 4$ in vrednostjo $\rho = 2$ nad 320-bitnim končnim obsegom, le-ta zagotavlja enako varnost, kot krivulja z vključitveno stopnjo $k = 8$ in vrednostjo $\rho = 1$ nad 160-bitnim obsegom. Implementacija točk na prvi krivulji zavzame dvakrat toliko prostora in aritmetika v končnem obsegu zahteva približno štirikrat več časa.

V splošnem je torej vrednost ρ tista, ki prevlada pri izbiri krivulje. Ni pa edini faktor, ki lahko vpliva na optimizacijo implementacije. Poleg vrednosti ρ je vredno izpostaviti še ovoje, ki smo jih opisali v razdelku 4.4. Tako bi hipotetična krivulja z vključitveno stopnjo $k = 6$ in vrednostjo $\rho = 4/3$ nad 214-bitnim obsegom $\mathbb{F}_q$ zagotavljala enako varnost, kot prejšnja primera. Če pa bi krivulja imela ovoj stopnje šest (glej razdelek 4.4), bi operacije v grupi lahko računali v obsegu $\mathbb{F}_q$ namesto v obsegu $\mathbb{F}_{q^k}$.

Če velikost podgrupe in obsega spremenimo, tako da nista nujno minimalne velikosti, lahko učinkovitost še izboljšamo. Kot primer vzemimo krivuljo z vključitveno stopnjo $k = 6$ in vrednostjo $\rho = 2$ nad 320-bitnim obsegom. Taka izbira parametrov več kot zadovolji varnostne zahteve, vendar pa je kljub temu lahko taka krivulja učinkovita, če ima ovoje stopnje šest. Splošno, če je $\rho \cdot k > b_2/b_1$, potem bo končni obseg večji od zahtevanega, če pa je $\rho \cdot k < b_2/b_1$, pa bo podgrupa večja od zahtevane.

7.9.2 Distorzijske preslikave

Večina parjenj v kriptografiji ima lastnost, da so izrojena, če so vhodni podatki (P, Q) linearno odvisni. Po drugi strani veliko protokolov zahteva, da so vhodni podatki iz iste ciklične grupe $\langle P \rangle$. Eden izmed načinov kako to preprečiti, je uporaba distorzijskih preslikav, ki smo jih spoznali v razdelku 5.5. Distorzijska preslikava obstaja za krivuljo E z vključitveno stopnjo $k > 1$ natanko tedaj, ko je E supersingularna [57, 149]. Primer, ko je $k = 1$ pa smo si ogledali v primeru konstrukcije 7.7.19.

Na navadnih krivuljah obstajajo drugi načini za reševanje problema izrojenosti in navadne krivulje se lahko uporabijo skoraj v vseh protokolih in shemah. Vendar je mnogokrat dokaz varnosti odvisen od eksistence distorzij in za take protokole je potrebno izbrati supersingularne krivulje, če želimo dokazljivo varnost [80]. Če pri tem upoštevamo zadnje rezultate s področja računanja diskretnega logaritma v končnh obsegih [1], zaradi katerih je uporaba supersingularnih krivulj varnostno vprašljiva, ostane odprto vprašanje, ali se da dokazljivo varnost dokazati tudi brez distorzij.

7.9.3 Ovoji in kompresija

Za navadne krivulje velja, da sta točki P in Q kot vhodna podatka za parjenja $e(P, Q)$ na eliptični krivulji z vključitveno stopnjo k iz grup $E(\mathbb{F}_q)$ oziroma $E(\mathbb{F}_{q^k})$ (glej razdelek 5.1). Če je k liho število, lahko uporabimo kvadratni ovoj in vzamemo točko Q na krivulji

$E'(\mathbb{F}_{q^{k/2}})$, kjer je E' kvadratni ovoj, ki smo ga spoznali v razdelku 4.4. Lastnost, da je k liho število je splošno zaželena, saj lahko pripomore k optimizaciji [8]. Še več, če je k deljiv s 6, je točka Q lahko na krivulji $E'(\mathbb{F}_{q^{k/6}})$, kjer je E' ovoj stopnje 6 [11].

Na vsaki eliptični krivulji z vključitveno stopnjo k, ki ima ovoj stopnje d, kjer $d \mid k$, je rezultat Tate-Lichtenbaumovega parjenja lahko element obsega $\mathbb{F}_{q^{k/d}}$ namesto $\mathbb{F}_{q^k}$. S tem prihranimo $\lceil \log_2 d \rceil$ bitov informacije. Ta kompresija sicer deluje samo na rezultatu parjenja, vendar se da podobno narediti tudi na celotnem parjenju nad primernim podobsegom obsega $\mathbb{F}_{q^k}$ [111].

Idealno bi bilo, če bi krivulja z vključitveno stopnjo k imela ovoj stopnje k, kar bi omogočalo, da bi bile vse točke na krivulji in vrednosti parjenja v osnovnem obsegu $\mathbb{F}_q$. Na žalost pa mora biti taka krivulja supersingularna ali pa mora bit njena vrednost ρ skoraj 2, kar je posledica naslednje trditve in izreka 4.8.10.

Trditev 7.9.1. *Če je E navadna eliptična krivulja nad obsegom $\mathbb{F}_q$ z vključitveno stopnjo $k > 1$ in ovojem stopnje k, potem je red podgrupe $r \leq 4\sqrt{q}$ in vrednost $\rho \geq 2 - \frac{4 \log 2}{\log r}$.* ■

Opomba: Iz izreka 4.8.10 in trditve 7.9.1 sledi, da ima vsaka navadna družina krivulj vrednost ρ vsaj 2 če ima:

- vključitveno stopnja $k = 6$ in diskriminanto $D = 3$ (konstrukcija 7.7.6);
- vključitvena stopnja $k = 4$ in diskriminanta $D = 1$ (konstrukcija 7.7.4);
- vključitvena stopnja $k = 2$ in poljubna diskriminanta (trditev 7.3.7).

7.9.4 Aritmetika v razširitvah obsega

Za določene vrednosti vključitvene stopnje $k \in \mathbb{N}$ se da aritmetiko v razširjenem obsegu $\mathbb{F}_{q^k}$ implementirati bolj učinkovito. Naj bo $d_1 < d_2 < \ldots < d_s = k,\ d_i \in \mathbb{N}$, kjer $d_i \mid d_{i+1}$ in naj bo $\mathbb{F}(q^{d_i})$ i-ta razširitev dobljena z dodajanjem korena polinoma $x^{d_i/d_{i-1}} + \beta_i$ za nek $\beta_i \in \mathbb{F}_{q^{d_{i-1}}}$, ki je dovolj majhen (da se ga predstaviti z malo biti). Če je obseg $\mathbb{F}(q^k)$ možno zgraditi kot stolp razširjenih obsegov

$$\mathbb{F}_q \subset \mathbb{F}_{q^{d_1}} \subset \mathbb{F}_{q^{d_2}} \subset \cdots \subset \mathbb{F}_{q^k},$$

potem se da aritmetiko učinkovit implementirati. Ta lastnost se bo bolj verjetno pojavila, če bo k oblike $2^a 3^b$ za neka $a, b \in \mathbb{N}_0$. Taki konstrukciji obsegov sta predstavila Koblitz in Menezes [81] ter Barreto in Naehrig [7].

7.9.5 Majhna Hammingova utež

Pri Millerjevem algoritmu za računanje parjenj, predstavljenim v razdelku 5.4 smo videli, da je število korakov odvisno od števila 1 v binarnem zapisu reda r, kar je **Hammingova utež** števila r, ki jo označimo s hw(r). Parjenje lahko izračunano hitreje, če je hw(r) majhna, Konstrukcija supersingularnih krivulj in krivulj po metodi Cocks-Pinch dovoljuje poljubno izbiro reda podgrupe r, zato lahko v teh primerih za r vzamemo praštevilo z majhno vrednostjo hw(r). Če je r dan s polinomom $r(x)$, kot smo to videli pri družinah, potem izbira x z majhno vrednostjo hw(x) lahko privede do velikosti reda r z majhno

varnost (v bitih)	$r(x)$ (v bitih)	$\max \deg(r)$
80	160	10
112	224	12
128	256	16
192	384	20
256	512	24

Tabela 7.10.1: Maksimalna stopnja $r(x)$ za različne varnostne zahteve

$\mathrm{hw}(r)$. Splošno je stopnja kontrole nad Hammingovo utežjo odvisna od stopnje polinoma $r(x)$ in ta kontrola je precej večja za polne družine, kot pa redke.

Če je Hammingova utež praštevilske velikosti obsega q majhna, tudi to vpliva na učinkovitost aritmetike, vendar moramo biti pri tem pazljivi, saj je diskretni logaritem za obsege $\mathbb{F}_q^*$ lažji zaradi učinkovitejšega algoritma [130].

7.10 Seznam vseh krivulj primernih za parjenje

V prejšnjih razdelkih smo si ogledali bistvene lastnosti parjenjem prijaznih krivulj, kako se take krivulje generirajo in kaj vse vpliva na implementacijo parjenj. Zdaj si bomo ogledali izbor krivulj za posamezne vrednosti parametrov. Faktorjev za izbor krivulje je precej. Najbolj pomembna sta želena stopnja varnosti v grupi na eliptični krivulji $E(\mathbb{F}_q)$ in v multiplikativni grupi $\mathbb{F}_{q^k}^*$. Vpliv na izbor krivulje pa ima tudi izbira parjenja uporabljenega v aplikaciji, zahteva za hitrost računanja in velikost v bitih. Seveda ne smemo zanemariti tudi dvomov glede posebnih krivulj in nenaključnih parametrov [78]. Tako bomo predstavili več različnih možnosti za izbiro eliptične krivulje.

Izbor krivulje poteka tako, da uporabnik najprej izbere minimalno velikost (v bitih) podgrupe in razširjenega obsega. Nato izbere metodo za generiranje krivulje iz tabele 7.10.2. Če izbrana konstrukcija generira redko družino krivulj, za iskanje eksplicitnih parametrov uporabi MNT metodo (glej razdelek 7.6.1). Če izbrana konstrukcije generira polno družino krivulj $(t(x), r(x), q(x))$, za izračun eksplicitnih parametrov uporabimo zanko po vseh $x \in \mathbb{Z}$, dokler ne najdemo take vrednosti x_0, da sta vrednosti $q(x_0)$ in $r(x_0)$ praštevili in vrednost $t(x_0)$ celo število. Če je stopnja polinomov velika glede na stopnjo zahtevane varnosti, je iskanje takega x_0 lahko zamudno [49]. Posledica zgornje ocene je, da stopnji polinomov $r(x)$ in $q(x)$ ne smeta biti preveliki, če za konstrukcijo krivulje uporabimo družino in želimo natančno definirati velikost podgrupe in obsega. Zahteva, da je $q(x)$ praštevilo, to še zaostri [49, razdelek 8].

V tabeli 7.10.1 so maksimalne vrednosti $\deg(r)$ za različne varnostne zahteve. Za vsako vrednost polinoma $r(x)$ velikosti $b+1$ v bitih, izračunamo vrednost d iz enakosti $2^{b/d}/(b^2 d \log 2) = 1$. Maksimalna vrednost $\deg(r)$ je malo večja od tako izračunanega d. Če smo lahko fleksibilni glede velikosti parametrov v bitih, potem x povečujemo dokler ne najdemo praštevili $q(x)$ in $r(x)$. Z malo sreče, bodo prve instance, kjer se bo to zgodilo, blizu želenih velikosti v bitih. Kljub temu pa pri $\deg(r) > 40$ pričakujemo malo praštevilskih vrednosti $r(x)$, ki so večja od 512 bitov, zato družine krivulj, z veliko stopnjo polinoma $r(x)$ niso priporočljive.

Primer. Naj bosta $q(x)$ in $r(x)$ polinoma generirana s konstrukcijo 7.7.6 in parametrom $k = 32$. Polinoma imata stopnji 34 in 32. Če želimo 512-bitno podgrupo praštevilskega reda, ki bo ekvivalentna glede varnosti 256-bitnem AES, nam pri izbiri $x = 66100$ polinom $q(x)$ da 543-bitno praštevilo in $r(x)$ 513-bitno praštevilo, kar je blizu našim zahtevanim velikostim. •

7.10.1 Priporočila

Priporočila temeljijo na [49] in so dopolnjena z novimi metodami. Odvisna so od več faktorjev.

Krivulje z vrednostjo $\rho \approx 2$

Če minimiziranje ρ ni zaželeno, potem je najbolj učinkovita Cocks-Pinch metoda (glej razdelek 7.5.1). Ta ima več prednosti:

- Deluje za poljubno vključitveno stopnjo k;
- Deluje za poljubno diskriminanto kompleksnega množenja (v mejah učinkovitosti $D < 10^{12}$);
- Praštevilski red r podgrupe $E(\mathbb{F}_q)$ je izbran vnaprej.

Edina ovira je v tem, da je vrednost ρ blizu 2, kar pomeni, da bo velikost opisa točke krivulje E v bitih približno dvakratnik minimalne velikosti v bitih zahtevane stopnje varnosti.

Krivulje z vrednostjo $\rho < 2$

Če uporabnik želi minimizirati vrednost ρ (recimo za zmanjšanje potrebne pasovne širine pri komunikaciji), potem so vrednosti za učinkovito implementacijo v tabeli 7.10.2. V njej so najboljše znane vrednosti ρ za družine krivulj z vključitveno stopnjo $k \leq 50$, ki naj bi pokrile vse želene stopnje varnosti. Za vsako vrednost k je v tabeli 7.10.2 dana najboljša vrednost ρ dosežena z dvema različnima konstrukcijama. Prva konstrukcija je tista, ki da najmanjšo vrednost ρ, če je diskriminanta kompleksnega množenja $D = 1$ ali $D = 3$. Enačbe krivulj za take primer so enostavno izračunljive. Če je $\gcd(q, 6) = 1$, so krivulje nad $\mathbb{F}_q$ dane z enačbama

$$\begin{aligned} E_1 :\ y^2 &= x^3 + ax \quad (D = 1), \\ E_2 :\ y^2 &= x^3 + b \quad (D = 3). \end{aligned}$$

V tabeli so za večine primerov najboljše vrednosti ρ dosežene s konstrukcijo 7.7.6, ostale konstrukcije se izkažejo pri manjših vrednostih k, $k \equiv 4 \pmod 6$ in vrednostih k, ki so deljive z 18. Vendar za krivulje z majhno diskriminanto kompleksnega množenja D obstajajo metode, ki pohitrijo Pollard rho algoritem [43]. Te metode sicer varnost znižajo samo za par bitov, vendar pa zbujajo dvome, da krivulje z majhno D niso varne. Zato so v tabeli 7.10.2 tudi najboljše vrednosti ρ za krivulje z variabilno D, dovoljene vrednosti D in konstrukcije, ki generirajo te vrednosti ρ.

Vse družine tabeli 7.10.2 se lahko uporabijo za generiranje krivulj, katerih vrednost ρ je zelo blizu vrednosti ρ družine. Vse družine z izjemo ene generirajo krivulje nad praštevilskimi obsegi in minimalni vključitveni obseg za te krivulje je $\mathbb{F}_{q^k}$. Edina izjema je supersingularna krivulja s $k = 3$. Minimalni vključitveni obseg za to krivuljo je ali $\mathbb{F}_{q^3}$ ali $\mathbb{F}_{q^{3/2}}$.

	fiksna $D \leq 3$				variabilna D			
k	ρ	D	deg(r)	Konstr./Raz.	ρ	D	deg(r)	Konstr./Raz.
1	$2,000$	3	2	K 7.7.6	$2,000$	poljubna	1	K 7.7.19
2	poljubna$^{\#}$	1,3	-	R 7.4.2	poljubna$^{\#}$	3 mod 4	-	R 7.4.2
3	**1,000**$^{\#}$	3	2	R 7.4.3	**1,000**	nekatere	2	R 7.6.1-7.6.2
4	$1,500$	3	4	K 7.7.10	**1,000**	nekatere	2	R 7.6.1-7.6.2
5	$1,500$	3	8	K 7.7.6	$1,500$	poljubna	4	K 7.8.6^{+}
6	$1,250$	1	4	K 7.7.18	**1,000**	nekatere	2	R 7.6.1-7.6.2
7	$1,333^{\dagger}$	3	12	K 7.7.6, 7.8.2^{+}	$1,333$	3 mod 4	12	K 7.8.2^{+}
8	$1,500$	3	8	K 7.7.6	$1,750$	poljubna	4	K 7.8.8
9	$1,333$	3	6	K 7.7.6	$1,833$	poljubna liha	12	K 7.7.2^{+}
10	$1,500$	1,3	8	K 7.7.5, 7.8.3^{+}	**1,000**	nekatere	4	R 7.6.4
11	$1,200$	3	20	K 7.7.6, 7.8.2^{+}	$1,200^{\dagger}$	3 mod 4	20	K 7.8.2^{+}
12	**1,000**	3	4	K 7.7.9	$1,750$	2 mod 8	8	K 7.7.7^{+}
13	$1,167^{\dagger}$	3	24	K 7.7.6	$1,250$	poljubna liha	24	K 7.7.2^{+}
14	$1,333^{\dagger}$	3	12	K 7.7.6	$1,500$	poljubna liha	12	K 7.7.3^{+}
15	$1,500$	3	8	K 7.7.6	$1,750$	poljubna soda	32	K 7.7.7^{*+}
16	$1,250$	1	8	K 7.7.18	$1,875$	poljubna	8	K 7.8.9
17	$1,125^{\dagger}$	3	32	K 7.7.13, 7.8.2^{+}	$1,188$	poljubna liha	32	K 7.8.2^{+}
18	$1,333$	3	6	K 7.7.14	$1,583$	2 mod 4	24	K 7.7.7^{+}
19	$1,111^{\dagger}$	3	36	K 7.7.6	$1,111^{\dagger}$	3 mod 4	36	K 7.8.2^{+}
20	$1,375$	3	16	K 7.7.6	$1,875$	poljubna	8	K 7.8.10
21	$1,333$	3	12	K 7.7.6	$1,792$	2 mod 4	48	K 7.7.7^{+}
22	$1,300^{\dagger}$	1	20	K 7.7.3	$1,300^{\dagger}$	poljubna liha	20	K 7.7.3^{+}
23	*1,091*†	3	*44*	*K 7.7.6, 7.8.2*$^{+}$	$1,091^{\dagger}$	3 mod 4	44	K 7.8.2^{+}
24	$1,250$	3	8	K 7.7.6	$1,875$	poljubna	8	K 7.8.11
25	$1,300^{\dagger}$	3	40	K 7.7.6	$1,350$	poljubna liha	40	K 7.7.2^{+}
26	$1,167^{\dagger}$	3	24	K 7.7.6, 7.8.3^{+}	$1,167^{\dagger}$	3 mod 4	24	K 7.8.3^{+}
27	$1,111$	3	18	K 7.7.6	$1,472$	2 mod 4	72	K 7.7.7^{+}
28	$1,333^{\dagger}$	1	12	K 7.7.4	$1,917$	6 mod 8	24	K 7.7.7^{*+}
29	*1,071*†	3	*56*	*K 7.7.6*	$1,107$	poljubna liha	56	K 7.7.2^{+}
30	$1,500$	3	8	K 7.7.6	$1,813$	2 mod 4	32	K 7.7.7^{+}
31	*1,067*†	3	*60*	*K 7.7.6, 7.8.2*$^{+}$	$1,067^{\dagger}$	3 mod 4	60	K 7.8.2^{+}
32	$1,063^{\dagger}$	3	32	K 7.7.6	-	-	-	-
33	$1,200$	3	20	K 7.7.6	$1,575$	2 mod 4	80	K 7.7.7^{+}
34	$1,125^{\dagger}$	3	32	K 7.8.3^{+}	$1,125^{\dagger}$	3 mod 4	32	K 7.8.3^{+}
35	*1,500*†	3	*48*	*K 7.7.6, 7.8.2*$^{+}$	$1,500^{\dagger}$	3 mod 4	48	K 7.8.2^{+}
36	$1,167$	3	12	K 7.7.16	$1,417^{\dagger}$	2 mod 8	24	K 7.7.7^{+}
37	*1,056*†	3	*72*	*K 7.7.6*	$1,083$	poljubna liha	72	K 7.7.2^{+}
38	$1,111^{\dagger}$	3	36	K 7.7.6	$1,167$	poljubna liha	36	K 7.7.3^{+}
39	$1,167$	3	24	K 7.7.6	*1,521*	*2* mod *4*	*96*	*K 7.7.7*$^{+}$
40	$1,375$	1	16	K 7.7.17	-	-	-	-
41	*1,050*†	3	*80*	*K 7.7.6, 7.8.2*$^{+}$	$1,075$	poljubna liha	80	K 7.7.2^{+}
42	$1,333$	3	12	K 7.7.6	$1,625$	2 mod 4	48	K 7.7.7^{+}
43	*1,048*†	3	*84*	*K 7.7.6, 7.8.2*$^{+}$	*1,048*†	*3* mod *4*	*84*	*K 7.8.2*$^{+}$
44	$1,150^{\dagger}$	3	40	K 7.7.6	$1,750$	6 mod 8	32	K 7.7.7^{*+}
45	$1,333$	3	24	*K 7.7.6*	*1,729*	*2* mod *4*	*96*	*K 7.7.7*$^{+}$
46	*1,136*†	1	*44*	*K 7.7.3*	$1,136^{\dagger}$	poljubna liha	24	K 7.7.3^{+}
47	*1,043*†	3	*92*	*K 7.7.6*	*1,043*†	*3* mod *4*	*92*	*K 7.8.2*$^{+}$
48	$1,125$	3	16	K 7.7.6	-	-	-	-
49	*1,190*†	3	*84*	*K 7.7.6*	*1,214*	*poljubna liha*	*96*	*K 7.7.2*$^{+}$
50	$1,300^{\dagger}$	3	40	K 7.7.6, 7.8.3^{+}	$1,300^{\dagger}$	3 mod 4	40	K 7.8.3†

Tabela 7.10.2: Priporočene konstrukcije eliptičnih krivulj z vključitveno stopnjo $k \leq 50$

Razlaga simbolov v tabeli 7.10.2:

- **krepko**: tako napisano vnosi v tabeli označujejo, da lahko konstruiramo eliptično krivuljo praštevilskega reda z dano vključitveno stopnjo.
- *ležeče*: označuje, da čeprav lahko dosežemo optimalne vrednosti ρ za dano družino, so stopnje vpletenih polinomov previsoke za praktično implementacijo. Za fiksno vrednost diskriminante D je zahteva za stopnjo polinoma $\deg(r) \leq 40$, za variabilne vrednosti diskriminante D je zahteva za stopnjo polinoma $\deg(r) \leq 80$. V primerih, ko je stopnja $\deg(r)$ prevelika, je najbolj uporabna Cocks-Pinch metoda, s katero dobimo krivulje z želeno vključitveno stopnjo in diskriminanto ter vrednostjo $\rho \approx 2$.
- †: vrednost ρ je iz [49] in je manjša od vrednosti ρ dobljene v [25];
- #: za vrednosti ρ so primerne supersingularne krivulje:
  - $k = 2$: za majhne D oziroma variabilne D lahko dobimo želene vrednosti ρ s supersingularnimi krivuljami (7.4.2). Odvisno od razreda ostankov $q \mod 12$, lahko konstruiramo krivulje z $D = 1,\ D = 3$ ali $D \equiv 3 \pmod 4$ z $(\frac{-D}{q}) = -1$ (algoritem 7.8.1). Če pa upoštevamo zadnje rezultate na področju računanja diskretnega logaritma [1], supersingularne krivulje niso primerne zato so zato edina alternative krivulje konstruirane po metodi Cocks-Pinch.
  - $k = 3$ in majhna vrednost diskriminante D: tudi tu je najbolj optimalna supersingularna krivulja nad obsegom $\mathbb{F}_{p^2}$ (7.4.3). Minimalni vključitveni obseg (obseg v katerem parjenja zavzamejo vrednosti) bo v tem primeru $\mathbb{F}_{p^6} = \mathbb{F}_{q^3}$, če je sled $t = p$ in $\mathbb{F}_{p^3} = \mathbb{F}_{q^{3/2}}$ če $t = -p$. Ker minimalni vključitveni obseg določa varnost diskretnega logaritma in ne vključitvena stopnja [66], je pri izbiri parametrov potrebna previdnost. Če je zahtevana krivulja nad praštevilskim obsegom, nam konstrukcija 7.7.6 da ustrezno družino z vrednostjo $\rho = 2$.
- $+$: osnovna navedena konstrukcija je kombinirana s substitucijo $x^2 \mapsto \alpha x^2$ v izreku 7.8.1.
- $*$: za $k = 15, 28, 44$ in variabilno diskriminanto D, se uporabijo iste tehnike kot v konstrukciji 7.7.7, edina razlika je tem, da se polinom $y(x)$, ki ustreza elementu obsega $(\zeta_k - 1)/\sqrt{-2}$, dodatno reducira po modulu $r(x)$. Polinomi za osnovno konstrukcijo so v tabeli 7.7.1.
- $-$: za dano vključitveno stopnjo k trenutno ne obstaja znana družina krivulj z majhno ali variabilno diskriminanto D. V teh primerih je najbolj uporabna Cocks-Pinch metoda, ki generira krivuljo z želeno stopnjo vključitve in diskriminanto ter vrednostjo $\rho \approx 2$.

Krivulje z učinkovito aritmetiko

V razdelku 7.9 smo spoznali nekaj tehnik za hitrejše računanje parjenj, ki so odvisne od vključitvene stopnje k, uporaba ovojev in konstrukcije razširjenih obsegov v stolpih. V tabeli 7.10.3 so krivulje, ki lahko izkoristijo obe tehniki. Vključitvene stopnje so oblike $k = 2^a 3^b,\ a, b \in \mathbb{N}_0$, saj ta izbira dovoljuje konstrukcijo razširjenih obsegov v stolpih. Če

k	ρ	D	Stopnja ovoja	Konstr. / Razd.
3	$1,000$	3	3	R 7.4.3
4	$2,000$	1	4	K 7.7.5
6	$2,000$	3	6	K 7.7.6
8	$1,500$	1	4	K 7.7.11
9	$1,333$	3	3	K 7.7.6
12	$1,000$	3	6	K 7.7.9
16	$1,250$	1	4	K 7.7.13
18	$1,333$	3	6	K 7.7.14
24	$1,250$	3	6	K 7.7.6
27	$1,111$	3	3	K 7.7.6
32	$1,125$	1	4	K 7.7.15
36	$1,167$	3	6	K 7.7.16
48	$1,125$	3	6	K 7.7.6

Tabela 7.10.3: Družine krivulj z učinkovito aritmetiko

je število k deljivo s 4, imajo krivulje z diskriminanto kompleksnega množenja $D = 1$ ovoj, ki se lahko uporabi za to, da računamo nad obsegom $\mathbb{F}_{q^{k/4}}$ namesto nad $\mathbb{F}_{q^k}$. Če je k deljiva s 3, imajo krivulje z diskriminanto kompleksnega množenja $D = 3$ ovoj, ki se lahko uporabi za računanje nad obsegom $\mathbb{F}_{q^{k/3}}$ če je k liho ali $\mathbb{F}_{q^{k/6}}$ če je k sodo.

Za vsak k manjši od 50, je v tabeli 7.10.3 seznam družin krivulj z ovojem najvišjega reda. Če je možnih več konstrukcij, izberemo tisto z najmanjšo vrednostjo ρ. Primeri za $k = 3, 4, 6$ so rezultat izreka 4.8.10, torej dejstva, da imajo krivulje z vključitveno stopnjo k in ovojem stopnje k ali $\rho \geq 2$ ali pa so supersingularne.

Poglavje 8

ZAKLJUČEK

V nalogi smo predstavili eliptične krivulje, pri čemer smo pot začeli pri algebraičnih raznoterostih. Opisali smo osnovne lastnosti eliptičnih krivulj ter delitelje, ki so nam omogočili vpeljati strukturo grupe točk na eliptični krivulji, kar je ključno za dobro razumevanje parjenj. Predstavili smo osnovne primere parjenj, ki se v uporabljajo v praksi, ter možne načine uporabe. Glavni del naloge je bil na enem mestu zbrati znane algoritme za konstrukcijo parjenjem prijaznih krivulj, ter raziskati kateri dejavniki vplivajo na varnost in učinkovito implementacijo. Tako je prispevek naloge poleg podrobnejše predstavitve eliptičnih krivulj in parjenj ter uporabe le-teh, dopolnjena taksonomija in zbrane najnovejše metode za konstrukcijo parjenjem prijaznih krivulj. Konstrukcije, ki so bile v obstoječi literaturi podane brez dokazov smo dokazali. Na seznam priporočljivih krivulj pa smo dodali konstrukcije za vključitvene stopnje $k = 8$, $k = 16$, $k = 20$ in $k = 24$, Naloga vsebuje tudi konkretne primere parjenjem prijaznih krivulj.

Tematika naloge je danes zelo aktualna in dinamična. Žal se parjenja velikokrat smatrajo kot črne škatle, saj povezujejo več področij matematike in zahtevajo predznanje klasične algebraične geometrije, teorije števil, algebre, če naštejemo le nekatera.

Zaradi zahtevnosti so parjenja implementirana v manjšem obsegu, kot bi zaradi uporabnosti lahko bila. S tem namenom smo v nalogi na elementaren način predstavili tudi nekaj osnovno teorijo in naredili tudi korak proti večjemu zaupanju v varnost.

Na samem področju je precej odprtih vprašanj. Na prvem mestu bi vsekakor izpostavili varnost supersingularnih krivulj, ki je v luči najnovejših rezultatov pri učinkovitem računanju diskretnega logaritma v razširitvah obsegov [1] vprašljiva. Mnogi avtorji zato supersingularnih krivulj ne priporočajo več. Tako so parjenja tipa 1, to so simetrična parjenja, v mnogih primerih označili kot neprimerna. Seveda se pojavi vprašanje, kakšne varnostne zahteve bi morale veljati in kako bi to vplivalo na hitrost, da bi bile krivulje še vedno primerne. Drugo vprašanje pa je, kako v obstoječih protokolih zamenjati supersingularne krivulje za navadne. Navkljub vsemu igrajo supersingularne krivulje vlogo v kriptosistemih, ki temeljijo na izogenijah in predstavljajo ključen člen v post-kvantni kriptografiji. Druga zanimiva tematika, so nove konstrukcije krivulj za vnaprej določene vključitvene stopnje. Pri trenutnih konstrukcijah smo omejeni predvsem z vrednostjo diskriminante, ki je poglavitna pri kreiranju krivulj z metodo kompleksnega množenja; posledično se pojavi vprašanje, ali obstaja kakšna boljša metoda za generiranje krivulj.

Poleg praktičnih odprtih vprašanj pa so odprta še teoretična, kot so: dokaz obstoja homomorfizma iz Verheulovega izreka, parjenja na raznoterostih in krivuljah višjega rodu,

obstoj preslikav podobnim distorzijam na navadnih krivuljah in dokazljiva varnost brez distorzij. Pomembna tema so tudi parjenja na krivuljah z vključitveno stopnjo enako 1, ki se lahko klasificirajo z dugačnimi metodami [29]. Ne smemo zanemariti tudi parjenja na krivuljah, kjer je red grupe točk sestavljeno število, ali pa je le ta vsebovana v večji grupi, katere red je deljiv z majhnim praštevilskim faktorjem [6].

Kot smo videli, je področje parjenj in iskanja posebnih krivulj odprto in zanimivo, tako da lahko v prihodnje pričakujemo nove rezultate.

Dodatek A

ALGEBRAIČNE STRUKTURE

V tem dodatku so predstavljene osnovne definicije in lastnosti iz teorije kvaternionov, obsegov, števil, polinomov in valuacij, ki jih srečujemo skozi celotno delo. Dokaze izrekov poleg drugih lastnosti in razlag najdemo v dodatnih referencah.

V nalogi privzemamo osnove teorije števil, kolobarjev in obsegov, ki so na voljo v [150]. Nanizali bomo le tiste, ki jih vseskozi uporabljamo.

A.1 Kvaternioni

Definicija A.1.1. Algebra $\mathcal{A}$ nad obsegom $\mathbb{Q}$ je vektorski prostor ali modul nad obsegom $\mathbb{Q}$ opremljen z notranjo operacijo $\otimes : \mathcal{A} \times \mathcal{A} \to \mathcal{A}$. **Red** O v algebri $\mathcal{A}$ nad $\mathbb{Q}$ je podkolobar kolobarja $\mathcal{A}$, ki je končno generiran kot $\mathbb{Z}$-modul in za katerega velja $O \otimes \mathbb{Q} = \mathcal{A}$.

Definicija A.1.2. Hamiltonovi kvaternioni so množica elementov oblike

$$H = \{a + bi + cj + dk : \ a, b, c, d \in \mathbb{Q}\},$$

kjer velja $i^2 = j^2 = k^2 = -1$ in $ij = k = -ji$.

Hamiltonovi kvaternioni sestavljajo nekomutativen kolobar, v katerem ima vsak neničelni element inverz.

Definicija A.1.3. Algebra kvaternionov je kolobar oblike

$$\mathcal{Q} = \{a + b\alpha + c\beta + d\alpha\beta : \ a, b, c, d \in \mathbb{Q}\},$$

kjer so $\alpha^2, \beta^2 \in \mathbb{Q}$, $\alpha^2 < 0$, $\beta^2 < 0$ in $\beta\alpha = -\alpha\beta$.

Definicija A.1.4. Maksimalni red O v algebri kvaternionov $\mathcal{Q}$ je podkolobar $\mathcal{Q}$, ki je končno generiran kot aditivna Abelova grupa in ima naslednjo lastnost: če je $\mathcal{R}$ kolobar, za katerega velja $O \subseteq \mathcal{R} \subseteq \mathcal{Q}$ in je $\mathcal{R}$ končno generiran kot aditivna Abelova grupa, potem je $O = \mathcal{R}$.

Kot primer maksimalnega reda si oglejmo Hamiltonove kvaternione. Podkolobar $\mathbb{Z} + \mathbb{Z}i + \mathbb{Z}j + \mathbb{Z}k$ je končno generirana aditivna Abelova grupa, ni pa maksimalni red, saj je vsebovan v

$$O = \mathbb{Z} + \mathbb{Z}i + \mathbb{Z}j + \mathbb{Z}\frac{1 + i + j + k}{2}.$$

Dejansko je tako definiran O kolobar in hkrati maksimalni red v H.

A.2 Obsegi

Definicija A.2.1. Ideal I kolobarja R je **praideal**, če velja $ab \in I \implies a \in I$ ali $b \in I$. **Celostno polje** je komutativen kolobar z enoto $e \neq 0$, za katerega velja $ab = 0 \implies a = 0$ ali $b = 0$.

Definicija A.2.2. Obseg je komutativen kolobar, v katerem ima vsak neničelni element inverz. Najmanjši obseg, ki vsebuje kolobar R, je **obseg ulomkov kolobarja** R sestavljen iz ekvivlenčnih razredov $\frac{a}{b}$ na naslednji način:

$$(a, b) \sim (a', b') \Leftrightarrow ab' = a'b,$$

za a, a' in neničelna b, b' iz kolobarja R. **Karakteristika obsega** K je najmanjše število $n \in \mathbb{N}$ za katero velja $n \cdot 1 = 0$. Če tako število ne obstaja, pravimo, da ima K karakteristiko 0. **Praobseg** je obseg, ki ne vsebuje nobenega netrvialnega podobsega.

A.2.1 Razširitve

Definicija A.2.3. Obseg F je razširitev obsega K, če velja $K \subseteq F$. Označimo jo z F/K. Naj bo F/K razširitev obsega K. Če obstaja tak element $\alpha \in F$, da je $F = K(\alpha)$, potem je α **primitivni element**.
Razširitev F/K obsega K je **algebraična**, če je vsak element razširitve algebraičen nad K, tj. vsak element razširitve je koren neničelnega polinoma s koeficienti v K.
Razširitev F/K je **razpadni obseg polinoma** $p(x) \in K$, če se $p(x)$ razcepi v linearne faktorje v F/K.
Razširitev F/K je **normalna**, če se vsak nerazcepni polinom v $K[x]$, ki ima korene v F, razcepi v linearne faktorje v F.
Razširitev F/K je **algebraično zaprtje** obsega K, če ima poljuben polinom iz $K[X]$ vse korene v obsegu F.

Razširitev F/K lahko gledamo tudi kot vektorski prostor F nad obsegom K.

Definicija A.2.4. Stopnja razširitve F/K označena z $[F : K]$ je dimenzija vektorskega prostora F nad obsegom K. Razširitev F/K je končna, če je $[F : K]$ končna.

Izrek A.2.5. *Vsaka končna razširitev F/K je algebraična.* ■

Definicija A.2.6. Razširitev F/K je **separabilna**, če je za vsak $a \in F$ njegov minimalni polinom nad K separabilen, tj. ima same različne ničle. Algebraična razširitev F/K je **Galoisova**, če je normalna in separabilna. **Galoisova grupa** $Gal_{F/K}$ je grupa vseh avtomorfizmov σ obsega F/K, za katere velja, da je $\sigma(k) = k$ za vsak $k \in K$.

Definicija A.2.7. Končna razširitev F/K obsega K s karakteristiko p je **čisto neseparabilna** (ang. purely inseparable), če za vsak $\alpha \in F$ obstaja $m > 0$, da velja $\alpha^{p^m} \in K$.

Definicija A.2.8. Obseg K je **popolni obseg** (ang. perfect field), če velja katerakoli izmed naslednjih lastnosti:

1. Vsak nerazcepen polinom nad obsegom K ima različne ničle;

2. Vsak nerazcepen polinom nad obsegom K je separabilen;

3. Vsaka končna razširitev obsega K je separabilna;

4. Vsaka algebraična razširitev obsega K je seprabilna;

5. Obseg K ima karakteristiko enako 0, ali pa je v primeru, ko je karakteristika enaka $p > 0$, vsak element obsega K p-ta potenca.

Izrek A.2.9.

1. *Vsak obseg karakteristike 0 je separabilen.*

2. *Naj bo F/K končna razširitev separabilnega obsega K. Potem obstaja primitivni element za razširitev F/K.*

■

Definicija A.2.10. Razširitev obsega K je **Abelova**, če je razširitev Galoisova z Abelovo Galoisovo grupo.

Končni obseg je obseg, ki vsebujejo končno elementov. Glavne lastnosti končnih obsegov so zajete v naslednjem izreku.

Izrek A.2.11. *Za vsako praštevilo p in naravno število n obstaja končni obseg s p^n elementi označen z $\mathbb{F}_{p^n}$. Vsak končni obseg s p^n elementi je izomorfen razpadnemu obsegu polinoma $x^{p^n} - x$ nad obsegom $\mathbb{F}_p$. Vsak končni obseg je izomorfen natanko enemu obsegu oblike $\mathbb{F}_{p^n}$.* ■

Ker so vsi končni obsegi oblike $\mathbb{F}_{p^n}$ za neko praštevilo p in naravno število n, v nalogi za označevanje končnih obsegov uporabljamo oznako $\mathbb{F}_q$, kjer je q potenca praštevila. Opazimo, da je $\mathbb{F}_p$ izomorfen $\mathbb{Z}/p\mathbb{Z}$ v katerem računamo po modulu p.

Definicija A.2.12. Naj bo F/K razširitev obsega K in naj bo $S \subset F$. S je **algebraično neodvisna množica** nad obsegom K, če za nobeno n-terico $s_1, \ldots, s_n \in S$ ne obstaja neničelni polinom $f \in K[x_1, \ldots, x_n]$ za katerega je $f(s_1, \ldots, s_n) = 0$.

Izrek A.2.13. *Za razširitev F/K veljata naslednji trditvi:*

1. *Naj bo F algebraičen nad $K(a_1, \ldots, a_n)$. Potem za algebraično neodvisno množico $\{b_q, \ldots, b_m\}$ velja $m \leq n$.*

2. *Vsaka razširitev F/K obsega K ima maksimalno algebraično neodvisno množico.*

■

Definicija A.2.14. Maksimalna algebraično neodvisna množica $S \subset F$ se imenuje **transcendentna baza** za F/K. **Transcendentna stopnja razširitve** F/K obsega K je moč transcendentne baze.

Na primer, transcendentna stopnja razširitve $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ je enaka 0, kajti $x^2 - 2 \in \mathbb{Q}[x]$.

A.2.2 Sledi in norme

Definicija A.2.15. Naj bo $\alpha \in F = \mathbb{F}_{q^m}$ in naj bo $K = \mathbb{F}_q$. **Sled** $Tr_{F/K}(\alpha)$ obsega K je definirana kot

$$Tr_{F/K}(\alpha) = \alpha + \alpha^q + \cdots + \alpha^{q^{m-1}}.$$

Če je obseg K podobseg obsega F in je hkrati praobseg (nima nobenega netrivialnega podobsega), potem sled $Tr_{F/K}(\alpha)$ imenujemo tudi **absolutna sled** elementa α in jo označimo kot $Tr_F(\alpha)$.

Definicija A.2.16. Naj bo $\alpha \in F = \mathbb{F}_{q^m}$ in $K = \mathbb{F}_q$. **Norma** $N_{F/K}(\alpha)$ elementa α nad obsegom K je definirana kot:

$$N_{F/K}(\alpha) = \alpha \cdot \alpha^q \cdot \cdots \cdot \alpha^{q^{m-1}} = \alpha^{(q^m-1)/(q-1)}.$$

A.2.3 Številski obsegi

Posebni primeri razširitev so **številski obsegi**. Več o številskih obsegih je na voljo v [79, 154]. Tu bomo predstavili osnove potrebne za razumevanje tematike v nalogi.

Definicija A.2.17. Številski obseg K je končna razširitev obsega $\mathbb{Q}$. Stopnja razširitve $[K : \mathbb{Q}]$ imenujemo tudi **stopnja** obsega K.

Posebna primera številskih obsegov sta kvadratni obseg (ang. quadratic field) in ciklotomični obseg (ang. cyclotomic field), ki si ju bomo v nadaljevanju tudi ogledali. Pred tem pa bomo navedli še nekaj osnovnih definicij in lastnosti številskih obsegov.

Definicija A.2.18. Algebraično celo število v številskem obsegu K je element $\alpha \in K$, ki je koren moničnega polinoma s koeficienti v $\mathbb{Z}$.

Če je K številski obseg stopnje n in $\alpha \in K$, potem obstaja linearna kombinacija $\{1, \alpha, \alpha^2, \ldots, \alpha^n\}$, saj je K n-dimenzionalen vektorski prostor nad $\mathbb{Q}$. Povedano drugače, obstaja tak polinom $f(X) \in \mathbb{Q}[X]$, da je $f(\alpha) = 0$. Elementu α pravimo **algebraično število**.

Definicija A.2.19. Minimalni polinom f algebraičnega števila α je monični polinom v $\mathbb{Q}[X]$ najmanjše stopnje, za katerega velja $f(\alpha) = 0$.

Trditev A.2.20.

1. *Minimalni polinom elementa $\alpha \in K$ ima celoštevilske koeficiente natanko tedaj, ko je α algebraično celo število.*

2. *Množica algebraičnih celih števil obsega $\mathbb{Q}$ je enaka $\mathbb{Z}$.*

■

Definicija A.2.21. Množico algebraičnih celih števil številskega obsega K označimo z O_K in jo imenujemo **kolobar celih števil** obsega K.

Izrek A.2.22. *Naj bo K številski obseg in $\alpha \in K$. Naslednji dve trditvi sta ekvivalentni:*

1. *α je algebraično celo število;*

2. *Abelova grupa* $\mathbb{Z}[\alpha] = \{a + b\alpha,\ a, b \in \mathbb{Z}\}$ *je končno generirana.*

■

Trditev A.2.23.

1. *Če je* K *številski obseg, potem je* O_K *kolobar.*

2. *Naj* K *številski obseg s kolobarjem* O_K*. Potem je* $\mathbb{Q} \cdot O_K = K$*.*

3. *Naj bo* K *številski obseg in* $\overline{K}$ *algebraično zaprtje. Nerazcepen polinom v* $K[X]$ *ne more imeti večkratne ničle v* $\overline{K}$*.*

4. *Naj bo* K *številski obseg in* L *končna razširitev obsega* K *stopnje* n*. Potem obstaja natanko* n *različnih monomorfizmov iz* L *v algebraično zaprtje* $\overline{K}$*.*

5. *Številski obseg* K *stopnje* n *nad* $\mathbb{Q}$ *ima* n *vključitev v* $\mathbb{C}$*.*

■

Pomembno orodje v teoriji številskih obsegov je teorija ramifikacije (ang. ramification theory). Podrobnosti in lastnosti pa so na voljo v [114, poglavje 3].

Definicija A.2.24. Naj bo $p \in \mathbb{Z}$ praštevilo in O kolobar celih števil. Ideal pO se razcepi v produkt praidealov $pO = \wp_1^{e_{\wp_1}} \cdots \wp_g^{e_{\wp_g}}$. [114, poglavje 2]. Če je $\wp$ praideal, ki vsebuje p, je **indeks ramifikacije** ideala $\wp$ enak eksponentu $e_\wp$ pri $\wp$ v razcepu pO. Pravimo, da je p **ramificiran**, če je $e_{\wp_i} > 1$ za nek i. V primeru $pO = \wp_1 \cdots \wp_g$ pa je p **neramificiran**.

Definicija A.2.25. Naj bo O kolobar celih števil, p praštevilo in f minimalni polinom elementa θ, za katerega velja $O = \mathbb{Z}[\theta]$. Pravimo, da p **ostane** praštevilo (ang. inert prime), če je pO praideal. V tem primeru imajo parametri iz zgornje definicije vrednosti $g = 1$, $e = 1$ in $f = n$. Pravimo, da je p **popolnoma ramificiran**, če je $g = 1, e = 1$ in $f = 1$.

A.2.4 Hilbertovi obsegi razredov

Definicija A.2.26. Grupa razredov (ang. Class group) CL številskega obsega K je definirana kot

$$CL(O_K) = I(O_K)/P(O_K),$$

kjer je $I(O_K)$ množica neničelnih idealov kolobarja celih števil O_K v K, $P(O_K)$ pa je množica glavnih idealov O_K.

Definicija A.2.27. Razširitev F/K je **neramificirana**, če noben element obsega K ni ramificiran v razširitvi. **Hilbertov obseg razredov** (ang. Hilbert class field) H/K je maksimalna neramificirana Abelova razširitev obsega K.

A.2.5 Kvadratni obsegi

Definicija A.2.28. Kvadratni obseg K je razširitev obsega $\mathbb{Q}$ stopnje 2.

Kvadratni obsegi so številski obsegi in glavni primeri kvadratnih obsegov so razširitve oblike $\mathbb{Q}(\sqrt{d})$, kjer $d \in \mathbb{Q}$ ni kvadrat kakega drugega elementa iz $\mathbb{Q}$. Take razširitve lahko definiramo tudi kot $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}[X]/(x^2-d)$. Ker d ni kvadrat, je polinom x^2-d nerazcepen nad $\mathbb{Q}$ in posledično je $\mathbb{Q}(\sqrt{d})$ res obseg. Obseg $\mathbb{Q}(\sqrt{d})$ lahko predstavimo kot podobseg v $\mathbb{C}$ in sicer preko injektivne preslikave $\mathbb{Q}[X]/(x^2-d) \to \mathbb{C}$. Kot smo omenili v A.2.23 sta taki vložitvi natanko 2 in sicer $\sigma_1 :\ a+bx \mapsto a+b\sqrt{d}$ in $\sigma_2 :\ a+bx \mapsto a-b\sqrt{d}$. Izkaže se, da so vsi kvadratni obsegi zgornje oblike, kar nam pove naslednji izrek.

Izrek A.2.29. *Naj bo K številski obseg stopnje 2. Potem je K izomorfen obsegu $\mathbb{Q}(\sqrt{d})$ za nek $1 \neq d \in \mathbb{Z}$ prost kvadratov.* ■

Kot smo videli zgoraj, so kvadratni obsegi oblike $\mathbb{Q}(\sqrt{d})$, kjer je d celo število prosto kvadratov. Posebni primeri kvadratnih obsegov so imaginarni kvadratni obsegi.

Definicija A.2.30. Naj bo $K = \mathbb{Q}(\sqrt{-d})$, kjer je $d > 0$ celo število prosto kvadratov. Tak kvadratni obseg K imenujemo **imaginarni kvadratni obseg**.

Kolobar algebraičnih celih števil O_K ima v takih primerih naslednjo obliko:

$$O_K = \begin{cases} \mathbb{Z}\left[\frac{1-\sqrt{-d}}{2}\right], & \text{če je } d \equiv 3 \pmod 4; \\ \mathbb{Z}[\sqrt{-d}], & \text{če je } d \equiv 1,2 \pmod 4; \end{cases} \tag{A.1}$$

kjer je $\mathbb{Z}[\delta] = \{a+b\delta,\ a,b \in \mathbb{Z}\}$.

Definicija A.2.31. Red (ang. order) v imaginarnem kvadratnem obsegu K je kolobar R z lastnostma $\mathbb{Z} \subset R \subseteq O_K$ in $\mathbb{Z} \neq R$.

Trditev A.2.32. *Red v imaginarnem kvadratnem obsegu $K = \mathbb{Q}(\sqrt{-d})$ je končno generirana Abelova grupa in ima obliko $R = \mathbb{Z} + \mathbb{Z}f\delta$, kjer je $f \in \mathbb{N}$ in $\delta = (1+\sqrt{-d})/2$ oziroma $\delta = \sqrt{-d}$ glede na zgornjo obliko O_K.* ■

Definicija A.2.33. Prevodnik f reda R je indeks reda R v O_K. **Diskriminanta reda** R pa je

$$D_R = \begin{cases} -f^2 d, & \text{če je } d \equiv 3 \pmod 4; \\ -4f^2 d, & \text{če je } d \equiv 1,2 \pmod 4. \end{cases} \tag{A.2}$$

Tako definirana diskriminanta D_R je diskriminanta kvadratnega polinoma, katerega koren je $f\delta$. Analogno za algebraično število β v $\mathbb{C}$ obstaja tako celo število $u \neq 0$, da je $u\beta$ algebraično celo število.

Pomembno orodje v teoriji kvadratnih obsegov so tudi binarne kvadratne forme. Tu bomo navedli samo potrebne definicije za razumevanje kompleksnega množenja v nalogi, ostalo je na voljo v [112].

Definicija A.2.34. Celoštevilska kvadratna forma v dveh spremenljivkah je $f(x,y) = ax^2 + bxy + cy^2$, kjer so $a, b, c \in \mathbb{Z}$. Kvadratna forma je **primitivna**, če so si a, b, c med seboj tuji. **Diskriminanta kvadratne forme** je $D = b^2 - 4ac$. Če je $D < 0$ je kvadratna forma **definitna**, drugače je **nedefinitna**. Celo število m **predstavlja** kvadratno formo, če ima enačba $f(x,y) = m$ celoštevilsko rešitev. Če je m pozitivno, pravimo da je forma **pozitivna**. Binarna kvadratna forma je **reducirana**, če velja naslednje:

1. Če je diskriminanta D negativna, je forma reducirana v primeru $|b| \leq a \leq c$;
2. Če je diskriminanta D pozitivna, je forma reducirana v primeru $\sqrt{D} - 2|c| < b < \sqrt{D}$.

Število razredov h_D reda kvadratnega obsega z diskriminanto $D < 0$ je enako številu reduciranih binarnih kvadratnih form z diskriminanto enako D.

Definicija A.2.35. Diskriminanta kompleksnega števila τ je diskriminanta $-D$ primitivne pozitivno definitne kvadratne forme $Q(x,y)$ z lastnostjo $Q(\tau, 1) = 0$.

Naslednja struktura je pomembna v teoriji števil in algebraični geometriji, mi bomo navedli zgolj definicijo.

Definicija A.2.36. [13]. Naj bo R red v imaginarnem kvadratnem obsegu $\mathbb{Q}(\sqrt{D})$ z diskriminanto $D < 0$. Potem je j-invarianta eliptične krivulje E/R algebraično celo število. Minimalni polinom inavariante j imenujemo **Hilbertov razredni polinom** in ga označimo z $H_D(x) \in \mathbb{Z}[x]$.

Hilbertov razredni polinom H_D za diskriminanto $D < 0$ je možno zapisati tudi kot $H_D(x) = \prod_\alpha (x - j(\alpha))$, kjer α teče po kompleksnih številih

$$\alpha = \frac{-b + \sqrt{D}}{2a},$$

za katere je $ax^2 + bxy + cy^2$ primitivna reducirana pozitivno definitna kvadratna forma z diskriminanto D, in $j(\alpha)$ funkcija definirana v (4.16) na strani 58.

A.2.6 Koreni enot, ciklotomični polinomi in obsegi

V tem razdelek si bomo ogledali razpadni obseg polinoma $x^n - 1$ nad poljubnim obsegom K za poljuben $n \in \mathbb{N}$. Hkrati bomo podali generalizirano definicijo korena enote.

Definicija A.2.37. Naj bo n naravno število. Razpadni obseg polinoma $x^n - 1$ nad obsegom K imenujemo **n-ti ciklotomični obseg nad** K in ga označimo s $K^{(n)}$. Korene polinoma $x^n - 1$ v $K^{(n)}$ imenujemo **n-ti koreni enote nad** K. Množico vseh takih korenov označimo z μ_n.

Lema A.2.38. *Če sta n in m naravni števili in n deli m, potem je $K^{(n)} \subseteq K^{(m)}$.* ■

Poseben primer definicije A.2.37 je v primeru $K = \mathbb{Q}$. V tem primeru je $K^{(n)}$ podobseg obsega kompleksnih števil in n-ti koreni enote so točke enakostraničnega n-kotnika na enotski krožnici z ogliščem v 1.

Za naše namene bodo najpomembnejši končni obsegi, vendar pa za osnovne lastnosti korenov enot ta predpostavka ni potrebna. Struktura μ_n je določena z z razmerjem med n in karakteristiko obsega p.

Izrek A.2.39. *Naj bo n naravno število in K obseg s karakteristiko p. Velja:*

1. *Če p ne deli n, potem je μ_n ciklična grupa reda n glede na množenje v obsegu $K^{(n)}$.*
2. *Naj bo n, $n = mp^e$, kjer je m naravno število in e in m nista deljiva s p. Potem velja $K^{(n)} = K^{(m)}$, $\mu_n = \mu_m$ in koreni $x^n - 1$ v $K^{(n)}$ predstavljajo m elementov v μ_m, vsakega z večkratnostjo p^e.*

■

Definicija A.2.40. Naj bo K obseg s karakteristiko p in n naravno število, ki ne deli p. Generator ciklične grupe μ_n imenujemo **primitivni n-ti koren enote** nad obsegom K.

Lema A.2.41. *Naj ζ_n označuje primitivni n-ti koren enote in $\mathbb{Q}(\zeta_n)$ obseg $\mathbb{Q}$ razširjen z ζ_n. Veljajo naslednje trditve.*

1. *Za vsako število $N \in \mathbb{Z}$ obstaja tako naravno število n, da je $\sqrt{N} \in \mathbb{Q}(\zeta_n)$.*
2. *Če je p praštevilo in $p \equiv 1 \pmod 4$, potem velja $\sqrt{p} \in \mathbb{Q}(\zeta_p)$.*
3. *Če je p praštevilo in $p \equiv 3 \pmod 4$, potem velja $\sqrt{-p} \in \mathbb{Q}(\zeta_p)$.*

■

Ker je μ_n končna ciklična grupa reda n, vsebuje $\varphi(n)$ različnih generatorjev, kjer je $\varphi(n)$ **Eulerjeva funkcija**, ki označuje število naravnih števil m, ki so tuja k n in $m \leq n$ [93, izrek 1.15]. To pomeni, da je natanko $\varphi(n)$ različnih primitivnih n-tih korenov enote v obsegu K. Če je ζ primitivni koren enote, potem so vsi ostali oblike ζ^s, kjer je s tuj k n in $1 \leq s \leq n$. Polinomi, katerih koreni so n-ti koreni enote, bodo za nas še posebej zanimivi.

Definicija A.2.42. Naj bo K obseg karakteristike p, n naravno število število, ki ni deljivo s p in ζ primitivni n-ti koren enote nad K. Polinomu

$$\Phi_n(x) = \prod_{\substack{s=1 \\ \gcd(s,n)=1}}^{n} (x - \zeta^s)$$

pravimo **n-ti ciklotomični polinom** nad obsegom K.

Polinom $\Phi_n(x)$ je neodvisen od izbire primitivnega korena enote ζ. Stopnja polinoma $\Phi_n(x)$ je $\varphi(n)$, koeficienti pa so elementi n-tega ciklotomičnega obsega nad K. V nadaljevanju bomo s $\prod_{d|n}$ označili produkt po vseh pozitivnih deliteljih d naravnega števila n vključno z 1 in n.

Izrek A.2.43. *Za obseg K karakteristike p in naravno število n, ki ni deljivo s p velja:*

1. $x^n - 1 = \prod_{d|n} \Phi_d(x)$;
2. *Koeficienti polinoma $\Phi_n(x)$ so elementi $\mathbb{Z}$ v primeru, da je pra-podobseg obsega K enak obsegu racionalnih števil. V nasprotnem primeru so koeficienti $\Phi_n(x)$ iz pra-podobsega v K.*

■

Primer. Naj bo r praštevilo in $k \in \mathbb{N}$. Potem je

$$\Phi_{r^k}(x) = 1 + x^{r^{k-1}} + x^{2r^{k-1}} + \cdots + x^{(r-1)r^{k-1}},$$

ker je po zgornjem izreku

$$\Phi_{r^k}(x) = \frac{x^{r^k} - 1}{\Phi_1(x)\Phi_r(x)\cdots\Phi_{r^{k-1}}(x)} = \frac{x^{r^k} - 1}{x^{r^{k-1}} - 1}.$$

Če je $k = 1$ je $\Phi_r(x) = 1 + x + x^2 + \cdots + x^{r-1}$. •

Definirajmo **Moebiusovo funkcijo** $\mu(n)$ na $\mathbb{N}$ kot

$$\mu(n) = \begin{cases} 1, & \text{če n=1;} \\ (-1)^k, & \text{če je n produkt k različnih praštevil;} \\ 0, & \text{če je n deljiv s kvadratom praštevila.} \end{cases}$$

Izrek A.2.44. *Naj bo K obseg karakteristike p in $n \in \mathbb{N}$, ki ni deljivo s p. Potem n-ti ciklotomični polinom Φ_n nad K zadošča naslednji enakosti:*

$$\Phi_n(x) = \prod_{d|n}(x^d - 1)^{\mu(n/d)} = \prod_{d|n}(x^{n/d} - 1)^{\mu(d)}.$$

■

Primer. Naj bo K obseg, nad katerim je definiran Φ_{12}. Velja:

$$\begin{aligned} \Phi_{12}(x) &= \prod_{d|12}(x^{12/d} - 1)^{\mu(d)} \\ &= (x^{12} - 1)^{\mu(1)}(x^6 - 1)^{\mu(2)}(x^4 - 1)^{\mu(3)} \cdot \\ &\quad (x^3 - 1)^{\mu(4)}(x^2 - 1)^{\mu(6)}(x - 1)^{\mu(12)} \\ &= \frac{(x^{12}-1)(x^2-1)}{(x^6-1)(x^4-1)} \\ &= x^4 - x^2 + 1. \end{aligned}$$

•

V nadaljevanju si bomo ogledali nekaj koristnih lastnosti ciklotomičnih obsegov.

Izrek A.2.45. *Ciklotomični obseg $K^{(n)}$ je enostavna algebraična razširitev obsega K. V posebnem velja:*

1. *Če je $K = \mathbb{Q}$, je ciklotomični polinom Φ_n nerazcepen nad K in $[K^{(n)} : K] = \varphi(n)$;*
2. *Za $K = \mathbb{F}_q$ in q tuj k n definirajmo $d \in \mathbb{N}$ kot najmanjše število z lastnostjo $q^d \equiv 1 \pmod{n}$. Potem Φ_n faktorizira v $\varphi(n)/d$ različnih moničnih nerazcepnih polinomov v $K[x]$ stopnje d. $K^{(n)}$ je razpadni obseg vsakega od teh nerazcepnih polinomov nad K in $[K^{(n)} : K] = d$.*

■

Primer. Naj bo $K = \mathbb{F}_{11}$ in naj bo $\Phi_{12}(x) = x^4 - x^2 + 1 \in \mathbb{F}_{11}[x]$. Po zgornjem izreku je $d = 2$ in $\Phi_{12}(x)$ faktorizira v $\Phi_{12}(x) = (x^2 + 5x + 1)(x^2 - 5x + 1)$, kjer sta oba faktorja nerazcepna v $F_{11}[x]$. Ciklotomični obseg $K^{(12)}$ je enak $\mathbb{F}_{121}$. •

Izrek A.2.46. *Končni obseg $\mathbb{F}_q$ je $(q-1)$-ciklotomični obseg nad katerimkoli od njegovih podobsegov.* ■

Ker je $\mathbb{F}_q^*$ multiplikativna ciklična grupa reda $q - 1$, za vsako pozitivno število n, ki deli $q - 1$, obstaja ciklična podgrupa $\{1, \alpha, \cdots \alpha^{n-1}\}$ grupe $\mathbb{F}_q^*$ reda n. Vsi elementi te podgrupe so n-ti koreni enote nad poljubnim podobsegom obsega $\mathbb{F}_q$ in generator α je primitivni n-ti koren enote nad poljubnim podobsegom obsega $\mathbb{F}_q$.

Lema A.2.47. *Naj bosta d in n naravni števili. Če d deli n in je n tuj k karakteristiki obsega, potem $\Phi_n(x)$ deli $(x^n - 1)/(x^d - 1)$.* ■

A.3 Rezultante in diskriminante polinomov

V tem razdelku bomo predstavili rezultante in diskriminant polinomov, ki jih potrebujemo v nalogi. Več o tem je na voljo v [85].

Definicija A.3.1. Rezultanta $\mathrm{Res}(f, g)$ polinomov f in g stopnje n in m je definirana kot

$$\mathrm{Res}(f, g) = a_0^m b_0^n \prod_{i,j} (\alpha_i - \beta_j),$$

kjer so α_i koreni polinoma $f(x) = a_0 x^n + \cdots + a_n$ in β_i koreni polinoma $g(x) = b_0 x^m + \cdots + b_m$.

Definicija A.3.2. Diskriminanta $\mathrm{Disc}(f)$ polinoma $f(x) = a_0 x^n + \cdots + a_n$ je definirana kot

$$\begin{aligned} \mathrm{Disc}(f) &= a_0^{2n-2} (-1)^{n(n-1)/2} \prod_{i \neq j} (\alpha_i - \alpha_j) \\ &= a_0^{2n-2} \prod_{i<j} (\alpha_i - \alpha_j)^2. \end{aligned}$$

Naslednje trditve opisujejo lastnosti polinomov, ki jih je možno dokazati s pomočjo rezultant in diskriminant [93]

Lema A.3.3. *Naj bo $L = \mathbb{Q}(\theta)$ številski obseg in naj bo $f(x)$ minimalni polinom θ. Potem je za vsak $\alpha \in L$ polinom $f(\alpha x^2)$ nerazcepen natanko tedaj, ko $\alpha\theta$ ni kvadrat v obsegu L.*
■

Trditev A.3.4. *Naj bo* $f(x) = \sum_{i=0}^{d} a_i x^i \in \mathbb{Z}[x]$ *nerazcepen in naj bo* α *celo število brez kvadratov, ki ne deli* $a_0 a_d \cdot \mathrm{Disc}(f)$. *Potem je* $f(\alpha x^2)$ *nerazcepen.* ■

Posledica A.3.5. *Naj bo* $k \in \mathbb{N}$ *in* α *celo število brez kvadratov z lastnostjo* $\alpha \nmid k$. *Potem je* $\Phi_k(\alpha x^2)$ *nerazcepen.*

A.4 Valuacije

Pri valuacijah in valuacijski kolobarjih se bomo omejili zgolj na osnovne lastnosti in definicije, povzete po [139].

Definicija A.4.1. Naj bo $K(V)$ obseg racionalnih funkcij raznoterosti V in naj bo $O \subset K(V)$ kolobar z naslednjima lastnostma:

1. $K \subsetneqq O \subsetneqq K(V)$;
2. Za vsak $f \in K(V)$ velja $f \in O$ ali $f^{-1} \in O$.

Kolobar O imenujemo **valuacijski kolobar**.

Izrek A.4.2. *Naj bo* O *valuacijski kolobar obsega funkcij* $K(V)$. *Velja naslednje:*

1. O *je lokalni kolobar; tj., vsebuje en sam maksimalni ideal* $P = O \setminus O^\times$, *kjer je* $O^\times = \{z \in O : \exists w \in O,\ wz = 1\}$ *grupa enot kolobarja* O;
2. *Naj bo* $f \in K(V)$ *neničelna funkcija. Potem je* $f \in P$ *natanko tedaj, ko je* $f^{-1} \notin O$;
3. *Za podobseg konstant* E *v* $K(V)$ *velja* $E \subseteq O$ *in* $E \cap P = \{0\}$.

■

Izrek A.4.3. *Za valuacijski kolobar* O *obsega funkcij* $K(V)$ *z maksimalnim idealom* P *velja:*

1. P *je glavni ideal;*
2. *Če je* $P = tO$, *potem ima vsak* $0 \neq f \in K(V)$ *obliko* $f = t^n u$ *za nek* $n \in \mathbb{Z}$ *in* $u \in O^\times$;
3. O *je celostno polje, v katerem je vsak ideal glavni.*

■

Definicija A.4.4. Kolobar, ki ima lastnosti iz izreka A.4.3, imenujemo **diskretni valuacijski kolobar**.

Definicija A.4.5. Diskretna valuacija obsega racionalnih funkcij $K(V)$ je funkcija $v : K(V) \to \mathbb{Z} \cup \{\infty\}$ z naslednjimi lastnostmi:

1. $v(f) = \infty \Leftrightarrow f = 0$;
2. $v(fg) = v(f) + v(g),\ \forall f, g \in K(V)$;

3. $v(f+g) \geq \min\{v(f), v(g)\},\ \forall f, g \in K(V)$;

4. Obstaja element $f \in K(V)$, za katerega je $v(f) = 1$;

5. $v(\alpha) = 0,\ \forall \alpha \in K,\ \alpha \neq 0$.

Za ∞, ki ni element v $\mathbb{Z}$, veljajo naslednje lastnosti: $\infty + \infty = \infty + n = n + \infty = \infty$ in $\infty > m$ za vsak $m \in \mathbb{Z}$.

V trditvi 3.2.1 obravnavamo lokalni kolobar raznoterosti v dani točki, ki je najpomembnejši primer diskretnega valuacijskega kolobarja v algebraični geometriji. Red točke v definiciji 3.2.3 pa je primer diskretne valuacije.

Dodatek B

PRIMERI KRIVULJ

V tem dodatku bomo predstavili nekaj konkretnih primeov krivulj, ki so generirane s pomočjo algoritmov opisanih v poglavju 7. Pri tem bo poudarek na krivuljah, ki so tudi dejansko implementirane v kakšni od prosto dostopnih knjižnic.

B.1 MNT krivulje

Družine, ki so jih izračunali Miyaji, Nakabayashi in Takano [107] so v tabeli B.1.1.

k	$q(x)$	$t(x)$	$r(x)$
3	$12x^2 - 1$	$-1 \pm 6x$	$12x^2 \pm 6x + 1$
4	$x^2 + x + 1$	$-x,\ x + 1$	$x^2 + 2x + 2,\ x^2 + 1$
6	$4x^2 + 1$	$1 \pm 2x$	$4x^2 \pm 2x + 1$

Tabela B.1.1: MNT družine krivulj

Primer.
Primeri MNT krivulj za $k = 6$ [116]:

- 160 bitna krivulja nad obsegom $\mathbb{F}_q$, kjer je

  $$q = 8C72D321E48AA1419B22F914CB43C112B76D7AE5.$$

  Enačba krivulje:

  $$E:\ y^2 = x^3 - 3x + b,$$

  kjer je

  $$b = 299CE219B7B01348FC2B5007B6AB1EE1005676F7.$$

  Red grupe je

  $$8C72D321E48AA1419B23B6B2E4A85A073822640F.$$

- 256 bitna krivulja nad obsegom $\mathbb{F}_q$, kjer je

  $$\begin{aligned} q \ &= \ F6529C2A424A6332B1D5054E2F7B68AA \\ &\quad EE7EF91874DD140C6919AF9B719ED905. \end{aligned}$$

Enačba krivulje:

$$E: \ y^2 = x^3 - 3x + b,$$

kjer je

$$\begin{aligned} b \ &= \ 6E974D68EF44F266AE3DD5D1F97C497C \\ &\quad 1D5452D1B074A6C06A25D4E5819CCD1C. \end{aligned}$$

Red grupe je

$$\begin{aligned} &F6529C2A424A6332B1D5054E2F7B68AB \\ &E99C585A8419AE9FB45C620E5EF666C3 \end{aligned}$$

- 307 bitna krivulja nad obsegom $\mathbb{F}_q$, kjer je

$$\begin{aligned} q \ &= \ 05F9732C02629855B99FD12895E6BDBE0BB706E \\ &\quad FA108E0C07AF66AAD00EB1F0F5989C33BD1C4E5. \end{aligned}$$

Enačba krivulje:

$$E: \ y^2 = x^3 - 3x + b,$$

kjer je

$$\begin{aligned} b \ &= \ 05607CD7395B5F49C34A289E4072C37A56601B6 \\ &\quad 9C8F64F6BA3F827C87DEE8279BC2E640F16C279. \end{aligned}$$

Red grupe je

$$\begin{aligned} &05F9732C02629855B99FD12895E6BDBE0BB706E \\ &D2F4DC3D3182475E37D3C9FA61B41FD46D6868F. \end{aligned}$$

-

B.2 GMT krivulje

Družine krivulj, ki so jih karakterizirali Galbraith, McKee in Valença [55]. Pri tem je potrebno upoštevati, da je $hr(x) = q(x) + 1 - t(x)$.

h	k	$q(x)$	$t(x)$	k	$q(x)$	$t(x)$	k	$q(x)$	$t(x)$
2	3	$8x^2+2x+1$ $56x^2+6x-1$ $56x^2+22x+1$	$-2x$ $-14x-2$ $-14x-4$	4	$8x^2+6x+3$	$-2x$	6	$8x^2+2x+3$ $24x^2+6x+1$	$2x+2$ $-6x$
3	3	$12x^2+8x+3$	$2x+1$	4	$12x^2+2x+3$ $12x^2+10x+5$ $60x^2+14x+1$ $60x^2+26x+3$ $60x^2+34x+5$ $60x^2+46x+9$	$2x+1$ $-2x$ $-10x-1$ $-10x-2$ $10x+3$ $10x+4$	6	$12x^2+4x+3$ $84x^2+16x+1$ $84x^2+128x+49$	$-2x+1$ $-14x-1$ $14x+11$
4	3	$16x^2+6x+3$ $48x^2+30x+5$ $112x^2+26x+1$ $112x^2+58x+7$	$-2x$ $6x+2$ $-14x-2$ $-14x-4$	4	$16x^2+14x+7$ $80x^2+38x+5$ $80x^2+58x+11$ $208x^2+54x+3$ $208x^2+106x+13$	$-2x$ $-10x-2$ $10x+4$ $-26x-4$ $26x+6$	6	$16x^2+10x+5$ $112x^2+54x+7$ $112x^2+86x+17$ $208x^2+30x+1$ $208x^2+126x+19$	$2x+2$ $14x+4$ $14x+6$ $-26x-2$ $-26x-8$
5	3	$20x^2+12x+5$ $140x^2+64x+7$ $140x^2+104x+19$ $260x^2+44x+1$ $260x^2+164x+25$ $380x^2+112x+7$ $380x^2+192x+23$	$2x+1$ $14x+3$ $14x+5$ $-26x-3$ $-26x-9$ $-38x-7$ $-38x-11$	4	$20x^2+2x+5$ $20x^2+18x+9$ $260x^2+74x+5$ $260x^2+126x+15$ $260x^2+134x+17$ $260x^2+186x+33$ $340x^2+46x+1$ $340x^2+114x+9$ $340x^2+226x+37$ $340x^2+294x+63$	$2x+1$ $-2x$ $-26x-4$ $26x+6$ $-26x-7$ $26x+9$ $-34x-3$ $34x+5$ $-34x-12$ $34x+14$	6	$20x^2+8x+5$ $60x^2+36x+7$ $140x^2+36x+3$ $140x^2+76x+11$ $260x^2+96x+9$ $260x^2+216x+45$ $380x^2+188x+23$ $380x^2+268x+47$	$-2x+1$ $6x+3$ $-14x-1$ $-14x-3$ $26x+5$ $26x+11$ $38x+9$ $38x+13$

Tabela B.2.1: GMT družine krivulj

Primer.
Primeri GMT krivulj za $k = 6$ in $h = 2$ [116]:

- 192 bitna krivulja nad obsegom $\mathbb{F}_q$, kjer je

  $$q = BF52ED99D5808F126790D7DC18D901B076429F3A2FA78F65.$$

  Enačba krivulje:

  $$E: \ y^2 = x^3 - 3x + b,$$

  kjer je

  $$b = 7EEAFAF4178E7349192E71FA4EB40C681A11A9B5B4F2C0C9.$$

  Red grupe je

  $$5FA976CCEAC0478933C86BEE93F2F8C16A54AE0A732FF4B5.$$

- 222 bitna krivulja nad obsegom $\mathbb{F}_q$, kjer je

  $q = 20DF589D615A00DE349A7B4179B6BA507C693FF8ECC83614A610AAC3.$

  Enačba krivulje:

  $$E: \ y^2 = x^3 - 3x + b,$$

  kjer je

  $b = 0F99D400C2C7DED3542EAA3662E551B389489A8D38C69EE1A818753F.$

  Red grupe je

  $106FAC4EB0AD006F1A4D3DA0BCDB24FB28F7F39C248E644D4FD14077.$

•

B.3 LMT krivulje

Družine krivulj, ki so jih s pomočjo algoritma 7.6.1 generirali Le, Mrabet in Tan [88].

h	k	$q(x)$	$r(x)$	$t(x)$	k	$q(x)$	$r(x)$	$t(x)$	k	$q(x)$	$r(x)$	$t(x)$
1	3	$3x^2-1$	$3x^2+3x+1$	$-3x-1$	4	x^2+x+1	x^2+2x+1	$-x$	6	x^2+1	x^2+x+1	$-x+1$
2	3	$2x^2+x+1$ $14x^2+3x-1$ $14x^2+17x+4$	x^2+x+1 $7x^2+5x+1$ $7x^2+5x+1$	$-x$ $-7x-2$ $7x+3$	4	$4x^2+2x+1$	$2x^2+2x+1$	$-2x$	6	$2x^2+x+2$ $6x^2+3x+1$	x^2+x+1 $3x^2+3x+1$	$-x+1$ $-3x$
3	3	$3x^2+2x+2$	x^2+x+1	$-x$	4	$3x^2+5x+5$ $15x^2+7x+1$ $15x^2+13x+3$	x^2+2x+2 $5x^2+4x+1$ $5x^2+6x+2$	$-x$ $-5x-1$ $-5x-2$	6	$3x^2+2x+3$ $9x^2+6x+2$ $21x^2+8x+1$ $21x^2+22x+6$	x^2+x+1 $3x^2+3x+1$ $7x^2+5x+1$ $7x^2+5x+1$	$-x+1$ $3x$ $-7x-1$ $7x+4$
4	3	$4x^2+3x+3$ $12x^2+9x+2$ $28x^2+13x+1$ $28x^2+27x+6$	x^2+x+1 $3x^2+3x+1$ $7x^2+5x+1$ $7x^2+5x+1$	$-x$ $-3x-1$ $-7x-2$ $7x+3$	4	$8x^2+6x+3$	$2x^2+2x+1$	$-2x$	6	$4x^2+3x+4$ $28x^2+13x+2$ $28x^2+27x+7$ $52x^2+15x+1$ $52x^2+41x+8$	x^2+x+1 $7x^2+5x+1$ $7x^2+5x+1$ $13x^2+7x+1$ $13x^2+7x+1$	$-x+1$ $-7x-1$ $7x+4$ $-13x-2$ $13x+5$
5	3	$5x^2+4x+4$ $35x^2+18x+2$ $35x^2+32x+7$ $65x^2+22x+1$ $65x^2+48x+8$ $95x^2+56x+7$ $95x^2+94x+22$	x^2+x+1 $7x^2+5x+1$ $7x^2+5x+1$ $13x^2+7x+1$ $13x^2+7x+1$ $19x^2+15x+3$ $19x^2+15x+3$	$-x$ $-7x-2$ $7x+3$ $-13x-3$ $13x+4$ $-19x-7$ $19x+8$	4	$5x^2+9x+9$ $25x^2+15x+3$ $25x^2+25x+7$ $65x^2+37x+5$ $65x^2+63x+15$ $85x^2+23x+1$ $85x^2+57x+9$	x^2+2x+2 $5x^2+4x+1$ $5x^2+6x+2$ $13x^2+10x+2$ $13x^2+10x+2$ $17x^2+8x+1$ $17x^2+8x+1$	$-x$ $-5x-1$ $-5x-2$ $-13x-4$ $13x+6$ $-17x-3$ $17x+5$	6	$5x^2+4x+5$ $15x^2+12x+4$ $35x^2+18x+3$ $35x^2+32x+8$ $65x^2+22x+2$ $65x^2+48x+9$ $95x^2+56x+8$ $95x^2+94x+23$	x^2+x+1 $3x^2+3x+1$ $7x^2+5x+1$ $7x^2+5x+1$ $13x^2+7x+1$ $13x^2+7x+1$ $19x^2+5x+3$ $19x^2+5x+3$	$-x+1$ $-3x$ $-7x-1$ $7x+4$ $-13x-2$ $13x+5$ $-19x-6$ $19x+9$
6	3	$6x^2+5x+5$ $18x^2+15x+4$ $78x^2+29x+2$ $78x^2+55x+9$ $114x^2+71x+10$ $114x^2+109x+25$ $126x^2+33x+1$ $126x^2+75x+10$	x^2+x+1 $3x^2+3x+1$ $13x^2+7x+1$ $13x^2+7x+1$ $19x^2+15x+3$ $19x^2+15x+3$ $21x^2+9x+1$ $21x^2+9x+1$	$-x$ $-3x-1$ $-13x-3$ $13x+4$ $-19x-7$ $19x+8$ $-21x-4$ $21x+5$	4	$12x^2+10x+5$ $60x^2+26x+3$ $60x^2+46x+9$ $102x^2+32x+2$ $102x^2+65x+10$	$2x^2+2x+1$ $10x^2+6x+1$ $10x^2+6x+1$ $17x^2+8x+1$ $17x^2+8x+1$	$-2x$ $-10x-2$ $10x+4$ $-17x-3$ $17x+5$	6	$6x^2+5x+6$ $18x^2+15x+5$ $42x^2+23x+4$ $42x^2+37x+9$ $78x^2+29x+3$ $78x^2+55x+10$	x^2+x+1 $3x^2+3x+1$ $7x^2+5x+1$ $7x^2+5x+1$ $13x^2+7x+1$ $13x^2+7x+1$	$-x-1$ $-3x$ $-7x-1$ $7x+4$ $-13x-2$ $13x+5$

Tabela B.3.1: LMT družine krivulj

B.4 BN krivulje

Vse krivulje so konstruirane v [11] na podlagi konstrukcije 7.7.9 in imajo obliko

$$E:\ y^2 = x^3 + 3,$$

z redom enakim n in Frobeniusov sledjo enako t. V vseh primerih je q praštevilo in $q \equiv 3 \pmod{}$ in $q \equiv 4 \pmod{9}$. Primer 256 bitne krivulje je implementiran tudi v prosto dostopnih knjižnicah [159, 160].

- 160 bitna krivulja z naslednjimi vrednostmi za q, n in t:

$$q = 1461501624496790265145448589920785493717258890819,$$

$$n = 1461501624496790265145447380994971188499300027613,$$

$$t = 1208925814305217958863207.$$

- 192 bitna krivulja z naslednjimi vrednostmi za q, n in t:

$$q = 6277101719531269400517043710060892862318604713139674509723,$$

$$n = 6277101719531269400517043709981664699904401744160036556389,$$

$$t = 7922816241420296879637953335.$$

- 224 bitna krivulja z naslednjimi vrednostmi za q, n in t:

$$q = 26959946667149205758383469736921695435015736735261155141423417423923$$

$$n = 26959946667149205758383469736921690242718878200571531029749235996909,$$

$$t = 5192296858534689624111674181427015.$$

- 256 bitna krivulja z naslednjimi vrednostmi za q, n in t:

$$\begin{aligned} q &= 115792089237314936872688561244471742058 \\ &\quad 375878355761205198700409522629664518163, \\ n &= 269599466671492057583834697369216 \\ &\quad 9024271887820057153102974923599690 9, \\ t &= 5192296858534689624111674181427015. \end{aligned}$$

B.5 TN krivulje

Vse krivulje so konstruirane v [145] na podlagi konstrukcije 7.7.12 in imajo obliko

$$E: \ y^2 = x^3 + ax,$$

z redom enakim n in Frobeniusov sledjo enako t. V vseh primerih je q praštevilo.

- 224 bitna krivulja z naslednjimi vrednostmi za a, q, n in t:

$$\begin{aligned} a &= 36300583600222330247585173239589466449560865688830 13 \\ &\quad 84405752660348790783773939211493518238200981612950 35, \\ q &= 72601167200444660495170346479178932899121731377660 27 \\ &\quad 68811505320697581567547878422987036476401963225900 69, \\ n &= 27205632000047130716160030618261 40 \\ &\quad 14808404525177076771934828454768 17, \\ t &= -11335680000014728504320006378939171360920909642914 60. \end{aligned}$$

- 256 bitna krivulja z naslednjimi vrednostmi za a, q, n in t:

$$\begin{aligned} a &= 10082750769548734299044899506169224168748842 \\ &\quad 63403670965649734798007425964980756397964097 \\ &\quad 62482157723155120808510796783952, \\ q &= 20165501539097468598089799012338448337497685268073 41 \\ &\quad 93129946959601485192996151279592819524964315446310 24 \\ &\quad 161702159356789, \\ n &= 11581614432149089047832789189966585476 3 \\ &\quad 90503326918594658592037634937230763121 7 \\ t &= -18892102362242321974058216300844394415164 29 \\ &\quad 1734047019380020. \end{aligned}$$

Literatura

[1] G. Adj, A. Menezes, T. Oliveira, F. Rodriguez-Henriquez, "Computing discrete logarithms in $\mathbb{F}_{3^{6\cdot 137}}$ and $\mathbb{F}_{3^{6\cdot 163}}$ using Magma", v *WAIFI 2014*, št. 9061, *Lecture Notes in Computer Science*, str. 3-22, Springer International, 2015.

[2] A.O.L. Atkin, F. Morain, "Elliptic curves and primality proving", *Mathematics of Computation*, št. 61, str. 29-68, 1993.

[3] A.K. Awasthi, L. Sunder, "ID-based Ring Signature and Proxy Ring Signature Schemes from Bilinear Pairings", *International Journal of Network Security*, št. 4, številka 2, str. 187–192, 2007 .

[4] D. Bailey, C. Paar, "Efficient arithmetic in finite field extensions with application in elliptic curve cryptography", *Journal of Cryptology*, št. 14, str. 153-176, 2001.

[5] R. Balasubramanian, N. Koblitz, "The improbability that an elliptic curve has subexponential discrete log problem under the Menezes-Okamoto-Vanstone algorithm", *Journal of Cryptology*, št. 11, str. 141-145, 1998.

[6] P.S.L.M. Barreto, C. Costello, R. Misoczki, M. Naehrig, G.C.C F. Pereira, G. Zanon, "Subgroup Security in Pairing-Based Cryptography", v *Progress in Cryptology – LATINCRYPT 2015*, št. 9230, *Lecture Notes in Computer Science*, str. 245-265, Springer International, 2015.

[7] P.S.L.M. Barreto, S. Galbraith, C. O'hEigeartaigh, M. Scott, "Efficient pairing computation on supersingular abelian varieties", *Designs. Codes and Cryptography*, št. 42, str. 239-271, 2007.

[8] P.S.L.M. Barreto, H.Y. Kim, B. Lynn, M. Scott, "Efficient algorithms for pairing-based cryptosystems", v *Advances in Cryptology—Crypto 2002*, št. 2442, *Lecture Notes in Computer Science*, str. 354-368, Springer, Berlin, 2002.

[9] P.S.L.M. Barreto, B. Lynn, M. Scott, "Constructing elliptic curves with prescribed embedding degrees", v *Security in Communication Networks—SCN 2002*, št. 2576, *Lecture Notes in Computer Science*, str. 263-273, Springer, Berlin, 2002.

[10] P.S.L.M. Barreto, B. Lynn, M. Scott, "On the selection of pairing-friendly groups", v *Selected Areas in Cryptography—SAC 2003*, št. 3006, *Lecture Notes in Computer Science*, str. 17-25, Springer, Berlin, 2003.

[11] P.S.L.M. Barreto, M. Naehrig, "Pairing-friendly elliptic curves of prime order", v *Selected Areas in Cryptography—SAC 2005*, št. 3897, *Lecture Notes in Computer Science*, str. 319-331, Springer, Berlin, 2006.

[12] P. Bateman, R. Horn, "A heuristic asymptotic formula concerning the distribution of prime numbers", *Mathematics of Computation*, št. 16, str. 363-367, 1962.

[13] J. Belding, R. Bröker, A. Enge, K. Lauter, "Computing Hilbert Class Polynomials", v *Algorithmic Number Theory, 8th International Symposium, ANTS-VIII Banff, Canada, May 17-22, 2008* , št. 5011, *Lecture Notes in Computer Science*, str. 282-295, Springer, Berlin, 2008.

[14] N. Benger, M. Charlemagne, D. Freeman, "On the security of pairing friendly abelaian varieties over non-primer fields", v *Pairing-Based Cryptography – Pairing 2009*, št. 5671, *Lecture Notes in Computer Science*, str. 52-65, Springer Berlin Heidelberg, 2009.

[15] H. Bidgloi et al., *Handbook of Information Security*, John Wiley & Sons, Inc, 2006.

[16] I.F. Blake, G. Seroussi, N.P. Smart, *Advances in Elliptic Curve Cryptography*, Cambidge University Press, 2005.

[17] I.F. Blake, G. Seroussi, N. Smart, *Elliptic Curves in Cryptography*, Cambidge University Press, 2005.

[18] D. Boneh, M. Franklin, "Identity-based encryption from the Weil pairing", v *Advances in Cryptology - CRYPTO 2001*, št. 2139, *Lecture Notes in Computer Science*, str. 213-229, Springer, Berlin, 2001.

[19] D. Boneh, C. Gentry, H. Shacham, B. Lynn, "Aggregate and verifiably encrypted signatures from bilinear maps", v *Advances in Cryptology - EUROCRYPT 2004*, št. 2656, *Lecture Notes in Computer Science*, str. 416-432, Springer, Berlin, 2004.

[20] D. Boneh, E.-J. Goh, K. Nissim, "Evaluating 2-DNF formulas on ciphertexts", v *Theory of Cryptography Conference—TCC 2005*, št. 3378, *Lecture Notes in Computer Science*, str. 325-341, Springer, Berlin, 2005.

[21] D. Boneh, B. Lynn, H. Shacham, "Short signatures from the Weil pairing", v *Advances in Cryptology - ASIACRYPT 2001*, št. 2248, *Lecture Notes in Computer Science*, str. 514–532, Springer, 2002.

[22] D. Boneh, K. Rubin, and A. Silverberg, "Finding composite order ordinary elliptic curves using the Cocks-Pinch method", *Journal of Number Theory*, št. 131 (5), str. 832-841, 2011.

[23] D. Boneh, M. Franklin, "Identity-based encryption from the Weil pairing", v *Advances in Cryptology – CRYPTO 2001*, št. 2139, *Lecture Notes in Computer Science*, str. 586-615, Springer, Berlin, 2001.

[24] W. Bosma, J. Cannon, C. Playoust, "The Magma algebra system. I. The user language", *Journal of Symbolic Computation*, št. 24(3-4), str. 235-265, 1997.

[25] F. Brezing, A. Weng, "Elliptic curves suitable for pairing based cryptography", *Designs ,Codes and Cryptography*, št. 37, str. 133-141, 2005.

[26] R. Bröker, *Constructing elliptic curves of prescribed order*, Ph.D. thesis, Dept. of Mathematics, Leiden University, 2006.

[27] R. Bröker, "Constructing Supersingular Curves", *Journal of Combinatorics and Number Theory 1*, št. 1, izdaja 3, str. 269-273, 2009.

[28] D.A. Buell, *Binary Quadratic Forms*, Classical Theory and Modern Computations, Springer-Verlag New York, 1989.

[29] S. Chatterjee, A. Menezes, F. Rodriguez-Henriquez, *On implementing pairing-based protocols with elliptic curves of embedding degree one*, Cryptology ePrint Archive Report 2016/403. https://eprint.iacr.org/2016/403.pdf.

[30] L. Chen, Z. Cheng, N.P. Smart, "Identity-based key agreement protocols from pairings", *International Journal of Information Security*, št. 6, str. 213-241, 2007.

[31] J. Chen, H.W. Lim, S. Ling, H. Wang, H. Wee, "Shorter IBE and Signatures via Asymmetric Pairings", v *Pairing-Based Cryptography – Pairing 2012*, št. 7708, *Lecture Notes in Computer Science*, str. 122-140, Springe, Berlin, 2013.

[32] Z. Cheng, M. Nistazakis, *Implementing Pairing-Based Cryptosystems*, Proceedings of IWWST-2005, London, UK, April 2005.

[33] J.C.Choon, J.H. Cheon, "An Identity-Based Signature from Gap Diffie-Hellman Groups", v *Public Key Cryptography — PKC 2003*, št. 2567, *Lecture Notes in Computer Science*, str. 18-30, Springer, Berlin, 2003.

[34] C. Cocks, R.G.E. Pinch, *Identity-based cryptosystems based on Weil pairing*, neobjavljen rokopis, 2001.

[35] H. Cohen, G. Frey, R. Avanzi, C. Doche, T. Lange, K. Nguyen, F. Vercauteren, *Handbook of Elliptic and Hyperelliptic Curve Cryptography*, CRC Press, 2005.

[36] A. Comuta, M. Kawazoe, T. Takahashi, "Pairing-friendly elliptic curves with small security loss by Cheon's algorithm", v *Information Security and Cryptography—ICISC 2007*, št. 4817, *Lecture Notes in Computer Science*, str. 297-308, Springer, Berlin, 2007.

[37] G. Cornell, J. Silverman, *Arithmetic Geometry*, Springer, New York, 1986.

[38] M. Deuring, "Die Typen der Multiplikatorenringe elliptischer Funktionenkörper", *Abh. Math. Sem. Hansischen Univ.*, št. 14, str. 197-272, 1941.

[39] *Digital Signature Standard (DSS)*, FIPS PUB 186-4, Federal Information Processing Standards Publication 186, National Institute of Standards and Tchnology, 2013.

[40] R. Dryło, "Constructing Pairing-Friendly Genus 2 Curves with Split Jacobian", v *Progress in Cryptology - INDOCRYPT 2012*, št. 7668, *Lecture Notes in Computer Science*, str. 431-453, Springer, Berlin, 2012.

[41] P. Duan, S. Cui, C.W. Chan, *Effective polynomial families for generating more pairing-friendly elliptic curves*, Cryptology ePrint Archive Report 2005/236. http://eprint.iacr.org/2005/236/.

[42] R. Dupont, A. Enge, F. Morain, "Building curves with arbitrary small MOV degree over finite prime fields", *Journal of Cryptology*, št. 18, str. 79-89, 2005.

[43] I. Duursma, P. Gaudry, F. Morain, "Speeding up the discrete log computation on curves with automorphisms", v *Advances in Cryptology—Asiacrypt 1999*, št. 1716, *Lecture Notes in Computer Science*, str. 103-121, Springer, Berlin, 1999.

[44] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms", *IEEE transactions on Infromation theory*, št. 31, str. 469-472, 1985.

[45] G. Fischer, *Plane Algebraic Curves*, Student Mathematical Library vol. 15, AMS 2001.

[46] D. Freeman, *Constructing Abelian Varieties for Pairing-Based Cryptography*, Ph.D. thesis, University of California, Berkely, 2008.

[47] D. Freeman, "Constructing pairing-friendly elliptic curves with embedding degree 10", v *Algorithmic Number Theory Symposium—ANTS-VII*, št. 4076, *Lecture Notes in Computer Science*, str. 452-465, Springer, Berlin, 2006.

[48] D. Freeman, "A generalized Brezing-Weng method for constructing pairing-friendly ordinary abelian varieties", v *Pairing-Based Cryptography—Pairing 2008*, št. 5209, *Lecture Notes in Computer Science*, str. 146-16, Springer, Berlin, 2008.

[49] D. Freeman, M. Scott, E. Teske, "A Taxonomy of pairing-friendly elliptic curves", *Journal of Cryptology*, št. 23(2), str. 224-280, 2010.

[50] D. Freeman, P. Stevenhagen, M. Streng, "Abelian varieties with prescribed embedding degree", v *Algorithmic Number Theory, ANTS VIII*, št. 5011, *Lecture Notes in Computer Science*, str. 60-73, Springer, Heidelberg, 2008.

[51] G. Frey, H. Rück, "A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves", *Mathematics of Computation*, št. 62, str. 865-874, 1994.

[52] W. Fulton, *Algebraic Curves*, Advanced Book Classics, Addison-Wesley, 1989.

[53] S.D. Galbraith, *Public Key Cryptography*, Cambridge University Press, 2012.

[54] S. Galbraith, P. Gaudry, "Recent progress on the elliptic curve discrete logarithm problem", *Designs, Codes and Cryptography*, št. 78, izdaja 1, str. 51-72, 2016.

[55] S. Galbraith, J. McKee, P. Valenç, "Ordinary abelian varieties having small embedding degre", *Finite Fields and their Applications*, št. 13, str. 800-814, 2007.

[56] S.D. Galbraith, K.G. Paterson, N.P. Smart, "Pairings For Cryptographers", *Discrete Applied Mathematics*, št. 156, izdaja 16, str. 3113-3121, 2008.

[57] S. Galbraith, V. Rotger, "Easy decision Diffie-Hellman groups", *LMS Journal of Computation and Mathematics*, št. 7, str. 201-218, 2004.

[58] S.D. Galbraith, "Supersingular Curves in Cryptography", v *Advances in Cryptology — ASIACRYPT 2001*, št. 2248, *Lecture Notes in Computer Science*, str. 495-513, Springer, Berlin, 2001.

[59] D. Hankerson, A.J. Menezes, S. Vanstone, *Guide to Elliptic Curve Cryptography*, Springer Professional Computing, 2004.

[60] R. Hartshorne, *Algebraic Geometry*, Springer-Verlag, 1977.

[61] J. Harris, *Algebraic Geometry: A first course*, Graduate text in mathematics, Springer-Verlag, New York, 1992.

[62] F. Hess, "Pairing lattices", v *Pairing-Based Cryptography — Pairing 2008*, št. 5209, *Lecture Notes in Computer Science*, str. 18-38, Springer, Berlin, 2008.

[63] F. Hess, *Exponent Group Signature Schemes and Efficient Identity Based Signature Schemes Based on Pairings*, IACR e-print archive. Avaliable from http://eprint.iacr.org/. 2002.

[64] F. Hess, "Efficient Identity Based Signature Schemes Based on Pairings", v *Selected Areas in Cryptography, 9th Annual International Workshop, SAC 2002*, št. 2595, *Lecture Notes in Computer Science*, str. 310-324, Springer, Berlin, 2003.

[65] F. Hess, N. Smart, F. Vercauteren, "The Eta pairing revisited", *IEEE Trans. Information Theory*, št. 52, str. 4595-4602, 2006.

[66] L. Hitt, "On the minimal embedding field", v *Pairing-Based Cryptography—Pairing 2007*, št. 4575, *Lecture Notes in Computer Science*, str. 294-301, (, S.pringer, Berlin, 2007), pp.

[67] D. Husemöller, *Eliptic Curves*, 2nd edn, GTM, vol. 111, Springer, 2004.

[68] A. Joux, "A one round protocol for tripartite Diffie-Hellman", *Journal of Cryptology*, št. 17, str. 263-276, 2004.

[69] A. Joux, K. Nguyen, "Separating decision Diffie-Hellman from computational Diffie-Hellman in cryptographic groups", *Journal of Cryptology*, št. 16, str. 239-247, 2003.

[70] E. Kachisa, *Constructing Brezing-Weng pairing friendly elliptic curves using elements in the cyclotomic field*, M.Sc. dissertation, Mzuzu University, 2007.

[71] E. Kachisa, E. Schaefer, M. Scott, "Constructing Brezing-Weng pairing friendly elliptic curves using elements in the cyclotomic field", v *Pairing-Based Cryptography—Pairing 2008*, št. 5209, *Lecture Notes in Computer Science*, str. 126-135, Springer, Berlin, 2008.

[72] K. Karabina, *On prime-order elliptic curves with embedding degrees 3, 4 and 6*, M.Math. thesis, Univ. of Waterloo, Dept. of Combinatorics and Optimization, 2006.

[73] K. Karabina, E. Teske, "On prime-order elliptic curves with embedding degrees 3, 4 and 6", v *Algorithmic Number Theory Symposium—ANTS-VIII*, št. 5011, *Lecture Notes in Computer Science*, str. 102-117, Springer, Berlin, 2008.

[74] K. Karabina, E. Knapp, A. Menezes, "Generalizations of Verheul's theorem to asymmetric pairings", *Advances in Mathematics of Communications*, št. 2, izdaja 1, str. 103-111, februar 2013.

[75] S. Kent, C. Lynn, K. Seo, "Secure border gateway protocole (Secure BGP)", *IEEE J. Selected Areas in Comm.*, št. 18(4), str. 582-592, April 2000.

[76] M.S. Kiraz, O. Uzunkol, *Still Wrong Use of Pairings in Cryptography*, Cryptology ePrint Archive, Report 2016/223. http://eprint.iacr.org/2016/223.

[77] N. Koblitz, "Elliptic curve cryptosystems", *Mathematics of Computation*, št. 48, str. 203–209, 1987.

[78] N. Koblitz, "Good and bad uses of elliptic curves in cryptography", *Moscow Mathematical Journal*, št. 2, str. 693-715, 2002.

[79] N. Koblitz, *A Course in Number Theory and Cryptography, 2nd ed*, Springer-Verlag, New York, 1994.

[80] N. Koblitz, A. Menezes, *Another look at "Provable Security"*, Technical report CORR 2004-20, Centre forApplice Cryptographic Research, University of Waterloo, Canada, 2004.

[81] N. Koblitz, A. Menezes, "Pairing-based cryptography at high security levels", v *Proceedings of Cryptography and Coding: 10th IMA International Conference*, št. 3796, *Lecture Notes in Computer Science*, str. 13-36, Springer, Berlin, 2005.

[82] E. Konstantinou, Y.C. Stamatiou, C. Zaroliagis, "On the Use of Weber Polynomials in Elliptic Curve Cryptography", v *First European PKI Workshop: Research and Applications, EuroPKI 2004, Samos Island, Greece, June 25-26, 2004*, št. 3093, *Lecture Notes in Computer Science*, str. 335-349, Springer, Berlin, 2004.

[83] M. Kraitchik, *Théorie des Nombres*, Vol. 1, Gauthier-Villars, Paris, 1922.

[84] S. Lang, *Elliptic Functions*, Springer, Berlin, 1987.

[85] S. Lang, *Algebra, revised 3rd edn*, Springer, Berlin, 2002.

[86] S. Lang, *Algebraic Number Theory*, Springer, New York, 1986.

[87] S. Lang, *Introduction to Algebraic and Abelian Functions, 2nd ed*, Springer, Berlin, 1982.

[88] D-P. Le, N. El Mrabet, C.H. Tan, "On Near Prime-Order Elliptic Curves with Small Embedding Degrees", v *Algebraic Informatics, 6th International Conference, CAI 2015, Stuttgart, Germany*, št. 9270, *Lecture Notes in Computer Science*, str. 140-151, Springer, Berlin, 2015.

[89] H-s. Lee, C-M. Park, "Constructing pairing-friendly curves with variable CM discriminant", *Bull. Korean Math. Soc.*, št. 49, izdaja 1, str. 75-88, 2012.

[90] A.K. Lenstra, "Unbelievable security: Matching AES security using public key systems", v *Advances in Cryptology—Asiacrypt 2001*, št. 2248, *Lecture Notes in Computer Science*, str. 67-86, Springer, Berlin, 2001.

[91] H.W. Lenstra, "Factoring integers with elliptic curves", *Annals of Mathematics*, št. 126, str. 649–673, 1987.

[92] H. W. Lenstra, "Solving the Pell Equation", *Algorithmic Number Theory, MSRI Publications*, št. 44, str. 1-23, 2008.

[93] R. Lidl, H. Niederreiter, *Finite fields*, Cambridge University Press, 2nd edition, 1997.

[94] F. Luca, D. Mireles, I. Shparlinski, "MOV attack in various subgroups on elliptic curves", *Illinois Journal of Mathematics*, št. 48, str. 1041-1052, 2004.

[95] F. Luca, I. Shparlinski, "Elliptic curves with low embedding degree", *Journal of Cryptology*, št. 19, str. 553-562, 2006.

[96] B. Lynn, *On the implementation of pairing-based cryptosystems*, PhD thesis, Stanford University, Stanford, California, 2005

[97] K. Matthews, "The Diophantine equation $x^2 - Dy^2 = N,\ D > 0$", *Expositiones Mathematicae*, št. 18, str. 323-331, 2000.

[98] B. Mazur, D. Goldfeld, "Rational isogenies of prime degree", *Inventiones mathematicae*, št. 44, izdaja 2, str. 129-162, 1978.

[99] K.S.McCurley, "Prime values of polynomials and irreducibility testing", *Bulletin (New Series) of the American Mathematical Society* , št. 11(1), str. 155-158, 1984.

[100] A. Menezes, "An introduction to pairing-based cryptography", *Recent Trends in Cryptography, edited by I. Luengo*, št. 477 Contemporary Mathematics, AMS-RSME, str. 47-65, 2009.

[101] A. Menezes, T. Okamoto, S. Vanstone, "Reducing elliptic curve logarithms to logarithms in a finite field", *IEEE Transactions on Information Theory*, št. 39, str. 1639-1646, 1993.

[102] A. Menezes, S. Vanstone, "Isomorphism classes of elliptic curves over finite fields of characteristic 2", *Utilitas Mathematica*, št. 38, str. 135-153, 1990.

[103] J. F. Mestre, *Lettre Adressee a Gaudry et Harley*, December 2000, http://www.math.jussieu.fr/∼mestre.

[104] V. Miller, "Use of elliptic curves in cryptography", v *Advances in Cryptology - CRYPTO 85*, št. 218, *Lecture Notes in Computer Science*, str. 417–426, Springer-Verlag, 1986.

[105] V. Miller, "The Weil pairing, and its efficient calculation", *Journal of Cryptology*, št. 17, str. 235-261, 2004.

[106] J.S Milne, *Complex Multiplication*, 2006

[107] A. Miyaji, M. Nakabayashi, S. Takano, "New explicit conditions of elliptic curve traces for FR-reduction", *IEICE Transactions on Fundamentals*, št. E84-A(5), str. 1234-1243, 2001.

[108] D. Moody, R. Peralta, R. Perlner, A. Regenscheid, A. Roginsky, L. Chen, "Report on Pairing-based Cryptography", *Journal of Research of the National Institute of Standards and Technology*, št. 120, str. 11-27, 2015.

[109] F. Morain, "Classes d'isomorphismes des courbes elliptiques supersingulières en caracteristique ≥ 3", *Utilitas Mathematica*, št. 52, str. 241-253, 1997.

[110] A. Murphy, N. Fitzpatrick, *Elliptic curves for pairing applications*, Cryptology ePrint Archive Report 2005/302.

[111] M. Naehrig, P.S.L.M. Barreto, P. Schwabe, "On compressible pairings and their computatio", v *Progress in Cryptology—Africacrypt 2008*, št. 5023, *Lecture Notes in Computer Science*, str. 371-388, Springer, Berlin, 2008.

[112] S.V. Neel, *Binary Quadratic Forms and the Ideal Class Group*, Lecture Notes, Harvard University, 2012.

[113] A. Odlyzko, "Discrete logarithms in finite fields and their cryptographic significance", v *Advances in Cryptology—Eurocrypt 1984*, št. 209, *Lecture Notes in Computer Science*, str. 224-314, Springer, Berlin, 1985.

[114] F. Oggier, *Algebraic Number Theory*, Lecture notes, Nanyang Technological University, 2009-2010.

[115] P.C. van Oorschot, M.J.Wiener, "Parallel collision search with cryptanalytic applications", *Journal of Cryptology*, št. 12, str. 1-18, 1999.

[116] D. Page, N. Smart, F. Vercauteren, "A comparison of MNT curves and supersingular curves", *Applivalbe Algebra in Engineering, Communication and Computing*, št. 17, str. 379-392, 2006.

[117] K. G. Paterson, "ID-based signatures from pairings on elliptic curves", *Electronics Letters*, št. 38, izdaja 18, str. 1025-1026, 2002.

[118] J. Plemelj, *Algebra in teorija števil*, SAZU, Ljubljana, 1962.

[119] S. Pohlig, M. Hellman, "An improved algorithm for computing discrete logarithms over GF(p) and its cryptographic significance", *IEEE Transactions on Information Theory*, št. 24, str. 106-110, 1978.

[120] J. Pollard, "Monte Carlo methods for index computation (mod p)", *Mathematics of Computation*, št. 32, str. 918-924, 1978.

[121] *Recommendation for Key Management - Part 1: General (Revision 3)*, NIST Special Publication 800-57, 2012.

[122] *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*, NIST Special Publication 800-56A Revision 2, 2013.

[123] R. Rivest, A. Shamir, Y. Tauman, "How to leak a secret", v *Proceedings of Asiacrypt 2001*, št. 2248, *Lecture Notes in Computer Science*, str. 552-565, Springer, Berlin, 2001.

[124] J. Robertson, *Solving the generalized Pell equation* $x^2 - Dy^2 = N$, Unpublished manuscript, 2004.

[125] H.G. Rück, "A note on eliptic curves over finite fields", *Mathematics of Computation*, št. 49, številka 179, str. 301-304, 1987.

[126] R. Sakai, K. Ohgishi, M. Kasahara, "Cryptosystems based on pairings", *2000 Symposium on Cryptography and Information Security - SCIS 2000*, Okinawa, Japonska, 2000.

[127] E. Schaefer, "A new proof for the non-degeneracy of the Frey-Rück pairing and a connection to isogenies over the base field", v *Computational Aspects of Algebraic Curves*, št. 13, *Lecture Notes Ser. Comput.*, str. 1-12, World Scientific, Singapore, 2005.

[128] A. Shamir, "Identity-based cryptosystems and signature schemes", v *Advances in Cryptology, Proceedings of CRYPTO 84*, št. 196, *Lecture Notes in Computer Science*, str. 47-53, Springer, Berlin, 1985.

[129] D. Schielzeth, M.E. Pohst, "On Real Quadratic Number Fields Suitable for Cryptography", *Experimental Mathematics*, št. 14, izdaja 2, str. 189-197, 2005.

[130] O. Schirokauer, "The number field sieve for integers of low weight", *Mathematics of Computation*, št. 79, str. 583-602, 2010.

[131] R. Schoof, "Elliptic curves over finite fields and the computation of square roots mod p", *Mathematics of Computation*, št. 44, str. 483-494, 1985.

[132] R. Schoof, "Counting points on elliptic curves over finite fields", *Journal de Theorie des Nombres de Bordeaux*, št. 7, str. 219-254, 1987.

[133] M. Scott, "Computing the Tate pairing", v *Topics in Cryptology—CT-RSA 2005*, št. 3376, *Lecture Notes in Computer Science*, str. 293-304, Springer, Berlin, 2005.

[134] M. Scott, "On the Efficient Implementation of Pairing-Based Protocols", v *Cryptography and Coding, 13th IMA International Conference, IMACC 2011*, št. 7089, *Lecture Notes in Computer Science*, str. 296-308, Springer, Berlin, 2011.

[135] M. Scott, P.S.L.M. Barreto, "Compressed pairings", v *Advances in Cryptology—Crypto 2004*, št. 3152, *Lecture Notes in Computer Science*, str. 140-156, Springer, Berlin, 2004.

[136] M. Scott, P.S.L.M. Barreto, "Generating more MNT elliptic curves", *Designs Codes and Cryptography*, št. 38, str. 209-217, 2006.

[137] J.H. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, GTM 106, 1986.

[138] J.H. Silverman, J. Tate, *Rational Points on Eliptic Curves*, Springer-Verlag, UTM, 1992.

[139] H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer-Verlag, GTM 254, 2009.

[140] H. Stichtenoth, C. Xing, "On the structure of the divisor class group of a class of curves over finite fields", *Archiv der Mathematik*, št. 65, Izdaja 2, str. 141-150, 1995.

[141] D.R. Stinson, *Cryptography, Theory and Practice*, CRC Press, 2nd edition, 2002.

[142] L. Su, H.W. Lim, S. Ling, H. Wang, "Revocable IBE Systems with Almost Constant-Size Key Update", v *Pairing-Based Cryptography – Pairing 2013*, št. 8365, *Lecture Notes in Computer Science*, str. 168-185, Springer, Berlin, 2014.

[143] A.V. Sutherland, "Computing Hilbert class polynomials with the Chinese Remainder Theorem", *Mathematics of Computation*, št. 80, str. 501-538, 2011.

[144] S. Tanaka, K. Nakamula, "Constructing pairing-friendly elliptic curves using factorization of cyclotomic polynomials", v *Pairing-Based Cryptography—Pairing 2008*, št. 5209, *Lecture Notes in Computer Science*, str. 136-145, Springer, Berlin, 2008.

[145] S. Tanaka, K. Nakamula, "More constructing pairing-friendly elliptic curves for cryptography", *Transactions of the Japan Society for Industrial and Applied Mathematics*, št. 17, str. 595-606, 2007.

[146] J. Tate, "Duality theorems in Galois cohomology over number fields", v *Proceedings of the International Congress of Mathematicians*, str. Djursholm: Inst. Mittag-Leffler, 1962.

[147] J. Tate, "Endomorphisms of abelian varieties over finite fields", *Inventiones Math.*, št. 2, str. 134-144, 1966.

[148] J. Tate, *WC-groups over p-adic fields*. Seminaire Bourbaki; 10e annee: 1957/1958, 13, Paris: Secretariat Mathematique

[149] E. Verheul, "Evidence that XTR is more secure than supersingular elliptic curve cryptosystems", *Journal of Cryptology*, št. 17, str. 277-296, 2004.

[150] I. Vidav, *Algebra*, DMFA - založništvo, Ljubljana, 2003.

[151] W.C. Waterhouse, "Abelian varietes over finite fields", *Annales scientifiques de l' École Norm. Sup.*, št. 4, str. 521-560, 1969.

[152] L.C. Washington, *Elliptic Curves: Number Theory and Cryptography*, CRC Press, 2nd edition, 2008.

[153] H. Weber, *Lehrbuch der Algebra*, Bd. 3, 2. Aufl . Braunschweig, 1908.

[154] T. Weston, *Algebraic Number Theory*, Lecture notes, Harvard, 1999.

[155] F. Zhang, K. Kim, "ID-Based Blind Signature and Ring Signature from Pairings", v *Advances in Cryptology — ASIACRYPT 2002* , št. 2501, *Lecture Notes in Computer Science*, str. 533-547, Springer, Berlin, 2002.

[156] F. Zhang, R. Safavi-Naini, W. Susilo, "An Efficient Signature Scheme from Bilinear Pairings and Its Applications", v *Public Key Cryptography – PKC 2004* , št. 2947, *Lecture Notes in Computer Science*, str. 277-290, Springer, Berlin, 2004.

[157] *http://www.larc.usp.br/∼pbarreto/pblounge.html*.

[158] *https://ellipticnews.wordpress.com/*

[159] *http://www.cipher.risk.tsukuba.ac.jp/tepla/*

[160] *https://github.com/relic-toolkit/relic.git*

[161] *https://crypto.stanford.edu/pbc/*